

ФГБОУ ВО  
«Уральский государственный юридический университет  
имени В. Ф. Яковлева»  
АНО «КримЛиб»  
Союз криминалистов и криминологов  
Проект «РИТВУС»

# **ТЕХНОЛОГИИ ХХІ ВЕКА В ЮРИСПРУДЕНЦИИ**

Материалы  
Шестой всероссийской  
научно-практической конференции  
(Екатеринбург, 24 мая 2024 года)



Екатеринбург  
2024

УДК 34  
ББК 67  
Т38

***Рецензенты:***

**И. Р. Бегишев** – доктор юридических наук, доцент, заслуженный юрист Республики Татарстан, главный научный сотрудник Научно-исследовательского института цифровых технологий и права, профессор кафедры уголовного права и процесса Казанского инновационного университета имени В. Г. Тимирязова

**А. А. Беляков** – доктор юридических наук, профессор, заведующий кафедрой криминалистики Уральского государственного юридического университета имени В. Ф. Яковлева

***Ответственный редактор:***

**Д. В. Бахтеев**, доктор юридических наук, доцент, профессор кафедры криминалистики Уральского государственного юридического университета имени В. Ф. Яковлева

**Т38** Технологии XXI века в юриспруденции: материалы Шестой всероссийской научно-практической конференции (Екатеринбург, 24 мая 2024 года) / отв. ред. Д. В. Бахтеев. — Екатеринбург: АНО «КримЛиб» — 2024. — 161 с. — 1 CD-ROM. — Систем. требования: 512 MB RAM; Windows XP/Vista/7/8/8.1/10/11; 4,89 Мб свобод. пространства на жест.диске. — Загл. с титул.экрана. — Текст: электронный.

ISBN 978-5-6049815-0-4

В сборнике представлены статьи учёных-юристов, представителей юридической практики и начинающих исследователей, принявших участие в Шестой всероссийской научно-практической конференции «Технологии XXI века в юриспруденции», посвящённой отдельным проблемам юридических науки и практики, связанным с современными технологиями.

Мнение авторов может не совпадать с мнением редакции.

УДК 34  
ББК 67

ISBN 978-5-6049815-1-1

© Авторы, 2024.

© АНО «Центр содействия развитию криминалистики  
«КримЛиб»»

© Уральский государственный  
юридический университет имени В. Ф. Яковлева, 2024

## Оглавление

Оглавление .....	3
<b>Арефинкина Екатерина Геральдовна</b>	
Цифровизация адвокатуры: необходимость или неизбежность? .....	5
<b>Бахтеев Дмитрий Валерьевич</b>	
Исследование выполнено за счёт гранта Российского научного фонда № 23-78-10011	
Векторы цифрового развития криминалистики.....	13
<b>Бекузарова Юлия Владимировна</b>	
Высокоавтоматизированные транспортные средства: основы правового регулирования .....	18
<b>Блинов Александр Георгиевич, Герасимов Александр Михайлович</b>	
Уголовно-правовая охрана генетической безопасности человечества в России .	23
<b>Галяшина Елена Игоревна</b>	
Переписка в мессенджерах как источник криминалистически значимой информации: особенности собирания и исследования .....	30
<b>Ганага Виктория Сергеевна</b>	
Следственные действия, проводимые посредством видео-конференц-связи, как источник получения доказательств.....	39
<b>Даниелян Армен Сергеевич</b>	
Адаптация юридического образования к цифровой эпохе: роль искусственного интеллекта.....	45
<b>Денисович Вероника Владимировна</b>	
Формирование концепции метавселенных в России .....	58
<b>Довгань Ксения Евгеньевна</b>	
Исследование выполнено за счёт гранта Российского научного фонда № 24-28-01400	
Проблемы толкования информационных правоотношений с точки зрения юридической казуистики.....	66
<b>Жевняк Оксана Викторовна</b>	
Правовой режим программно-аппаратных комплексов .....	69
<b>Зуев Сергей Васильевич</b>	
Информационно-технологический процесс уголовного судопроизводства: вопрос времени.....	77
<b>Иванов Владислав Юрьевич, Янкевич Екатерина Алексеевна</b>	
Личность несовершеннолетнего киберпреступника как элемент криминалистической характеристики преступлений.....	83

**Караваева Анастасия Владимировна**

Теоретико-правовые основы применения IT-технологий в системе профилактики преступлений ..... 87

**Коваленко Наталья Евгеньевна**

Вызовы информационных отношений современности как фактор развития правовых категорий: на примере субъекта права ..... 91

**Леднёв Илья Валерьевич**

Исследование выполнено за счёт гранта  
Российского научного фонда № 23-78-10011

Проблемы учёта по механизму преступления ..... 94

**Перевозникова Екатерина Юрьевна**

Современное состояние правового регулирования преступлений в сфере информационно-телекоммуникационных технологий ..... 102

**Рябчиков Сергей Александрович**

Электронный документооборот как центральное звено цифровой платформы уголовного судопроизводства..... 109

**Семенова Евгения Викторовна**

Электронное уголовное дело: понятие и перспективы внедрения в уголовный процесс России ..... 115

**Сергеев Алексей Михайлович**

Обзор источников правового регулирования использования автономных транспортных средств..... 123

**Хамидуллин Руслан Сибгатуллович**

Криминалистическое обеспечение раскрытия и расследования преступлений с использованием технологий искусственного интеллекта ..... 131

**Цветкова Анна Денисовна**

Исследование выполнено за счёт гранта  
Российского научного фонда № 23-78-10011

Проблемные аспекты определения исполнителя напечатанного текста ..... 136

**Шевырталов Егор Павлович**

Современные технологии обработки информации, используемые при расследовании краж и угонов автомобилей ..... 142

**Щербаков Игорь Олегович, Ужегов Максим Васильевич**

Интернет вещей как источник криминалистически значимой информации..... 148

**Яковлева Кристина Юрьевна**

Возможности применения технологии «блокчейн» в уголовном процессе ..... 154

**Арефинкина Екатерина Геральдовна**  
Кандидат юридических наук, заведующая кафедрой  
уголовного права и процесса,  
Юридический факультет Сочинского института  
Российского университета дружбы народов имени Патриса Лумумбы  
(г. Сочи, Российская Федерация)  
arefinkina@mail.ru

## **ЦИФРОВИЗАЦИЯ АДВОКАТУРЫ: НЕОБХОДИМОСТЬ ИЛИ НЕИЗБЕЖНОСТЬ?**

**Аннотация:** В статье рассматривается процесс развития цифровизации адвокатуры в современном обществе. Автор выделяет основные нововведения в деятельности адвокатуры в результате внедрения электронных технологий. Рассматриваются и анализируются как положительные, так и отрицательные стороны цифровизации адвокатуры, Комплексной информационной системы адвокатуры России. В статье отмечается, что цифровизация направлена на упрощённое взаимодействие между правоохранительными, судебными органами и адвокатом, влияет на профессиональное взаимодействие адвоката с доверителем, где новые «компетенции» и возможности адвоката позволяют отслеживать информацию о ходе рассмотрения дела, знакомиться с судебными актами. Делается вывод о том, что в настоящее время цифровизация адвокатуры не сможет активно работать без взаимодействия и цифровизации самой правоохранительной и судебной системы.

**Ключевые слова:** адвокатура, цифровизация, судопроизводство, адвокатская тайна, адвокатская палата.

Процесс цифровизации в последние годы набирает всё большие темпы во многих отраслях нашей жизни. Не осталась в стороне и сфера адвокатской деятельности. Но у любого научно-технического прогресса всегда есть две стороны. Безусловно, новейшие технологии открывают множество возможностей. Так, адвокату стало значительно проще знакомиться с материалами дела, делая сразу фотографии нужных документов и в нужном количестве. Сейчас намного проще с помощью электронных систем отследить назначение и движение дела; ознакомиться с последними поправками в действующее законодательство, а также, нажав одну кнопку, сопоставить старые редакции закона с новыми; просмотреть судебную практику не только в своём, но и любом другом регионе по интересующему вопросу, найти нужный судебный акт или образец необходимого процессуального документа и т. д. Это то, что пришло на смену выпискам из материалов уголовных дел, вклеиванию последних поправок в бумажный вариант кодекса, «Справочнику адвоката» с образцами документов, без которого в былые годы так сложно было

сориентироваться быстро, как надлежит оформлять тот или иной документ. Но, безусловно, тотальная цифровизация сферы юриспруденции может привести к тому, что в профессиональной сфере адвокаты будут соперничать не друг с другом, а с компьютерами и искусственным интеллектом, а этот «бой», вероятнее всего, окажется неравным. Уже сейчас часть традиционных консультативных услуг оказалась невостребованной, так как обыватель многое находит самостоятельно в информационно-телекоммуникационных сетях, по-своему интерпретирует, оформляет и использует для защиты своих прав, а заодно, порой, и чужих, создавая этим немало сложностей как себе, так и соответствующим структурам, куда он с вновь полученными знаниями обращается, искренне недоумевая тому, почему образование юриста невозможно получить на двухмесячных курсах.

Новые технологии незаменимы в рутинной работе, связанной с обработкой большого количества информации, сбором данных и их анализом, рассылкой типовой корреспонденции разным адресатам с получением подтверждений её доставки или отсутствием возможности для вручения, подготовкой типовых судебных документов и пр. Безусловно, передача рутинных функций автоматизированным системам – это лучший способ экономии человеческих и денежных ресурсов. Но в то же время имеется большая вероятность того, что эта часть юридической деятельности будет в дальнейшем полностью заменена машинным трудом.

Снижение спроса на юридические услуги – мировая тенденция. Однако всё не так однозначно. Чтобы оценить, какие угрозы для будущего юридической профессии и адвокатуры, в частности, несёт цифровизация, нужно понимать, что именно она из себя представляет в этой сфере на данный момент времени. Одним из наиболее известных проявлений цифровизации юридической деятельности является LegalTech, что в переводе с английского языка дословно означает «правовые технологии». Получается, что право, трансформируясь в цифровом пространстве, превращается и выражается в нём в юридических технологиях, которые должны иметь под собой законное правовое основание и обоснование<sup>1</sup>. Обобщённо LegalTech подразумевает использование всевозможных сервисов, которые оптимизируют рабочие процессы юристов, а также информационных технологий, онлайн-сервисов и специального программного обеспечения для повышения эффективности юридической деятельности.

Наиболее известным широкому пользователю и давно вошедшим в практику примером информационных технологий в юриспруденции являются справочные правовые системы, такие как «КонсультантПлюс», «Гарант», «Кодекс» и т. д. Активно на практике стали применяться такие инструменты, как электронные сервисы подбора судебной практики, составления договоров, калькулятор госпошлины, неустоек, сервис «Мой арбитр», а также некоторые иные специализированные платформы для юристов. Подробное освещение данного вопроса может в будущем стать предметом отдельной научной статьи.

---

<sup>1</sup> Савенко Н. Е. Legaltech в цифровой экономике и правовом регулировании экономической деятельности граждан // Право. Журнал Высшей школы экономики. 2023. Т. 16. № 1. С. 152.

В рамках же настоящей работы необходимо остановиться на том, какие цифровые технологии уже вошли в сферу адвокатской деятельности или могут войти в ближайшей перспективе.

В рамках проводимой цифровой трансформации института адвокатуры в апреле 2024 г. на законодательном уровне был закреплён статус Комплексной информационной системы адвокатуры России (далее – КИС АР) как автоматизированной системы, предназначенной для комплексной автоматизации деятельности Федеральной палаты адвокатов РФ, региональных адвокатских палат, адвокатских образований и адвокатов<sup>2</sup>. На нормативном уровне определено, что вышеуказанная система предназначена для информационного взаимодействия с другими структурами в форме единой системы межведомственного электронного взаимодействия. Цель КИС АР – обеспечение «цифровой трансформации (цифровизации) определённых бизнес-процессов и функций, связанных с осуществлением адвокатской деятельности и функционированием адвокатской корпорации (включая управление ею)»<sup>3</sup>. В настоящее время данная система продолжает совершенствоваться, в её подсистему планируется включить в том числе и финансовый блок оплаты труда адвокатов по назначению, который с помощью новых технологий позволит сделать эту сферу адвокатской деятельности верифицируемой, прозрачной и доступной.

По мнению Е. Г. Авакян, вице-президента Федеральной палаты адвокатов РФ, цифровая независимость адвокатуры как составная часть принципа её независимости включает создание цифровых продуктов за счёт собственных средств адвокатуры и закрепление результатов на праве собственности (например, КИС АР), что исключает влияние государства и иных органов на создание и оборот новых цифровых продуктов при внедрении их в деятельность адвокатуры<sup>4</sup>.

Первый вице-президент Федеральной палаты адвокатов РФ Михаил Толчеев констатировал, что на сегодняшний день около 80 % регионов подключены к подсистеме автоматизированного распределения поручений на защиту по назначению Комплексной информационной системы адвокатуры России (АРПН КИС АР), которая недавно получила нормативное закрепление в Федеральном законе «Об адвокатской деятельности и адвокатуре в Российской Федерации». Принятие закона, по его мнению, является эпохальным событием, так как оно открывает дорогу к интеграции платформы адвокатуры с судебными, следственными и иными государственными платформами в сфере правоприменения, что, в частности, ведёт к созданию прозрачной системы

---

<sup>2</sup> Федеральный закон от 22.04.2024 № 83-ФЗ «О внесении изменений в Федеральный закон “Об адвокатской деятельности и адвокатуре в Российской Федерации”» // СПС «Консультант Плюс» [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_475019/](https://www.consultant.ru/document/cons_doc_LAW_475019/) (дата обращения: 02.06.2024).

<sup>3</sup> Гаврилов С. Н. Об отдельных терминах в области цифровой трансформации адвокатской деятельности и адвокатуры // Адвокатская практика. 2022. № 5. С. 43–50.

<sup>4</sup> Авакян Е. Г. Принципы адвокатуры при ее преобразовании в условиях цифровой трансформации // Адвокатская практика. 2024. № 1. С. 7.

оплаты дел по назначению, даёт возможность направления адвокатского запроса в электронном виде и формирования цифрового ордера адвоката, моментально поступающего следователю или в суд<sup>5</sup>. Вышеуказанную систему рассматривают как средство от так называемых «карманных» адвокатов. Правоохранители больше не могут вызывать тех, с кем им удобно работать. Процедура стала электронной: заявка отправляется в систему, программа распределяет дела произвольно.

Система КИС АР в сфере адвокатской деятельности будет и дальше развиваться и модернизироваться, так как пока она направлена на совершенствование работы адвокатов в сфере уголовного производства и исключительно по назначению. Однако для этого необходимо активнее внедрять в адвокатуре электронный документооборот; заботиться о безопасности тех сведений, которые попадают в адвокатском сообществе в цифровую среду, так как адвокат является носителем адвокатской тайны и несёт за её сохранение ответственность в соответствии с действующим законодательством. Вероятнее всего, в перспективе развитие цифровой среды в адвокатуре будет происходить за счёт последовательного включения в систему КИС АР новых сервисов: ведение делопроизводства (для адвокатов, образований и палат), обучение и повышение квалификации, внесение оплаты, уплаты взносов, ведение адвокатских производств и пр.<sup>6</sup> В перспективе, адвокат сможет через свой личный кабинет осуществлять работу во многих направлениях более мобильно и ряд действий проводить дистанционно. Правовое регулирование цифровой трансформации адвокатуры должно охватывать как внутреннюю её организацию (гл. 4 ФЗ «Об адвокатской деятельности и адвокатуре»), так и внешнюю сторону новых отношений<sup>7</sup>.

Адвокаты без всяких сомнений должны оптимизировать свои процессы, а это без применения современных технологий невозможно. Следовательно, работа адвоката в ближайшей перспективе будет становиться всё более технологичной. Это избавит адвокатское сообщество от рутинной работы и исключит свойственные человеку ошибки. Технологии позволяют не только анализировать прошлое и настоящее, но и определять будущее. На основе анализа больших данных адвокат в будущем сможет, например, строить свои стратегии ведения конкретного дела или принимать решение о разрешении спора в досудебном порядке. Дополнительно можно будет избежать правовых ошибок и описок при формировании важных процессуальных решений, поскольку автоматизированная система в меньшей степени подвержена риску их

---

<sup>5</sup> Прозрачность системы гарантирует искоренение карманных адвокатов // Федеральная палата адвокатов Российской Федерации [Электронный ресурс]. 17 мая 2024. URL: <https://fparf.ru/news/media/prozrachnost-sistemy-garantiruet-iskorenenie-karmannykh-advokatov/> (дата обращения: 20.05.2024).

<sup>6</sup> Распределение будущего: что ждать от цифровизации адвокатуры? // Сфера [Электронный ресурс]. 20 октября 2020. URL: <https://legalacademy.ru/sphere/post/raspredelenie-buduschego-cto-zhdet-ot-cifrovizacii-advokatury> (дата обращения: 20.04.2024).

<sup>7</sup> Авакян Е. Г. Понятие адвокатуры и адвокатской деятельности при их цифровой трансформации // Адвокатская практика. 2023. № 4. С. 5.



допущения. Однако, полагаем, что только взаимодействие человеческого интеллекта и компьютерных алгоритмов способно вывести процесс аналитики и принятия решений в сфере адвокатской деятельности на новый уровень. Цифровизация – это лишь средство. Без человеческой эрудиции, опыта, даже при наличии необходимых технических средств она безжизненна. Кроме того, «автоматизация анализа информации вовсе не означает автоматизацию принятия решений на основе этой информации»<sup>8</sup>. Человеческий надзор за аналитической деятельностью искусственного интеллекта необходим, причём осуществлять такой контроль должны высокопрофессиональные специалисты со стажем и опытом. Именно такими специалистами являются адвокаты, получившие свой статус в установленном законом порядке, прошедшие соответствующий профессиональный и образовательный отбор, повышающие свою квалификацию на постоянной основе.

Вместе с тем, адвокаты имеют гуманитарное образование, а значит, информационные технологии зачастую им чужды и любые процессы автоматизации воспринимаются скептически или даже негативно. Однако стоит согласиться с мнением о том, что сами по себе цифровые технологии не угрожают в будущем адвокатской деятельности. Там, где деятельность адвоката форматизирована, часть работы вполне можно поручить интеллектуальной платформе. Адвокатская деятельность нередко требует вдумчивой аналитики, рассмотрения вопросов с точки зрения морали и нравственности и пр.<sup>9</sup> Однако совершенно очевидно, что в шаблонных и типовых операциях человека давно может и должен заменить компьютер. Человек нужен там, где ситуация предполагает многовариантность и обилие критериев самого разного характера, оценить которые машине пока затруднительно. Поэтому во все времена, при любом развитии цифровизации на первом месте всегда будет мастерство адвоката<sup>10</sup>.

В современных условиях нужно говорить об изменении содержания труда адвоката. Появление новых требований к адвокатской деятельности и новых компетенций, прежде всего в области компьютерных и информационных технологий, а также новых методов организации юридической работы – это те реальные изменения адвокатской профессии, которые происходят уже сейчас, и удельный вес которых будет нарастать в ближайшее время. Современный адвокат должен разбираться в информационных технологиях, использовать их в своей профессиональной деятельности и уметь с их помощью регулировать правовые отношения. Цифровая трансформация адвокатуры – это не столько количественные изменения (хотя они, несомненно, есть и будут), связанные с числом востребованных адвокатов, доходностью адвокатской деятельности или

---

<sup>8</sup> Демиденко Д. Робот-адвокат: как юристам не остаться без работы // Forbes [Электронный ресурс]. 24 апреля 2017. URL: <https://www.forbes.ru/kompanii/343269-robot-advokat-kak-yuristam-ne-ostatsya-bez-raboty> (дата обращения: 12.05.2024).

<sup>9</sup> Мрастьева О.С., Семикина С.А. К вопросу о развитии цифровизации и ее влиянии на адвокатуру // Адвокатская практика. 2023. 3 3. С. 2.

<sup>10</sup> Володина С. И. Электронное досье по уголовному делу в эпоху цифровизации // Адвокатская практика. 2021. № 2. С. 27.

распространённостью в обществе адвокатских услуг, сколько качественные, связанные с изменением содержания и форм организации профессиональной адвокатской деятельности. Адвоката будет тяжело представить без ИТ-помощников: систем, обрабатывающих значительные объёмы информации, автоматически анализирующих судебную практику, подбирающих возможные аргументы для усиления позиции стороны в суде и формирующих простые договорные документы. Сейчас много сил уходит на поиск и анализ нужной информации, отслеживание изменений в законодательстве и судебной практике по различным источникам, а в будущем фокус внимания адвоката должен переместиться в область управления юридическими рисками.

Можно с уверенностью сказать, что сегодняшнему адвокату следует иметь базовые знания в сфере юридических технологий. Представляется, что молодых адвокатов надо сразу учить пользоваться информацией – и это важнее штудирования законов; учить ориентироваться в развивающихся цифровых условиях: в новом программном обеспечении, аналитических технологиях и платформах отчётности; осваивать несвойственные юриспруденции сферы знаний, чтобы быть конкурентоспособным в профессии; приобретать навыки в сфере новых технологий, в том числе сбор доказательств в сети, обеспечение кибербезопасности, электронное делопроизводство и др. Однако остаётся дискуссионным вопрос: до какого уровня надо погружаться адвокату в цифровые технологии, чтобы избежать в будущем «ловушки компьютеризации»<sup>11</sup>, ведь можно уже с грустью констатировать, что сегодня наблюдается реальный дефицит не искусственного, а естественного интеллекта.

В заключении можно хотелось бы сформировать ряд общих положений, рекомендаций, связанных с неизбежностью цифрового генезиса адвокатуры, который повлечёт необходимость развития соответствующих компетенций представителями адвокатского сообщества:

1. Цифровую трансформацию нужно осуществлять уже сегодня. Автоматизация адвокатской деятельности – объективная реальность, не зависящая от желания представителей профессионального сообщества. Её основное направление – автоматизация рутинной работы. Тот, кто не начнет пересматривать свои возможности в этой сфере в ближайшее время может оказаться неконкурентоспособным.

2. Цифровая трансформация – не только внедрение новых технологий, но, что гораздо важнее, это обучение в сфере цифровых технологий, их реальное применение на практике, формирование культуры использования продукта.

3. Данные – большая ценность. Повсеместное внедрение электронных баз данных и в перспективе систем на основе искусственного интеллекта в адвокатской деятельности потребует анализа и загрузки большого объёма качественных данных, в том числе архивных. Уже сегодня нужно думать о том,

---

<sup>11</sup> Согомонян А. Юрист будущего: заучивать законы и кодексы больше нет нужды? // ИПС «Гарант.ру» [Электронный ресурс]. 15 ноября 2017. URL: <https://www.garant.ru/article/1148675/> (дата обращения: 02.06.2024).

как эту информацию защитить от неправомерного использования и избежать её утечки в случае хакерских атак или системных сбоев.

Воздействие цифровых технологий на отрасли права – это не просто «модная тема», которая со временем исчезнет, а важное направление развития юридической практики. Можно выделить следующие важные компетенции, которые необходимо развивать молодым адвокатам и уже сложившимся специалистам:

- 1) междисциплинарность и конструктивное взаимодействие со специалистами из других областей;
- 2) освоение новых юридических технологий, расширение знаний и навыков в сфере цифровизации, повышение цифровой грамотности;
- 3) непрерывное образование, профессиональная подготовка и переподготовка.

Следует согласиться с Н. Айрапетян, что цифровизация – это необходимость для современного адвоката, и цифровой скачок учит всех новым навыкам, позволяет обрести новые компетенции. Угрозу может представлять лишь неправильный подход к процессу адаптации правовой системы и юридических процессов к новым реалиям<sup>12</sup>.

Адвокат цифровой эпохи – человек, способный работать не только в реальном, но и виртуальном пространстве. У сегодняшней адвокатуры есть два варианта: придерживаться своей традиционной функции или активно и творчески взаимодействовать с меняющейся средой, совершенствоваться вместе с меняющейся реальностью.

### Список литературы:

1. Авакян Е. Г. Принципы адвокатуры при ее преобразовании в условиях цифровой трансформации // Адвокатская практика. 2024. № 1. С. 2–7.
2. Авакян Е. Г. Понятие адвокатуры и адвокатской деятельности при их цифровой трансформации // Адвокатская практика. 2023. № 4. С. 2–5.
3. Айрапетян Н. Творчество в профессии адвоката через призму новых технологий: возможна ли тотальная цифровизация с учетом специфики адвокатской деятельности? // Адвокатская газета [Электронный ресурс]. 27 октября 2022. URL: <https://www.advgazeta.ru/mneniya/tvorchestvo-v-professii-advokata-cherez-prizmu-novykh-tekhnologiy/> (дата обращения: 02.06.2024).
4. Володина С. И. Электронное досье по уголовному делу в эпоху цифровизации // Адвокатская практика. 2021. № 2. С. 23–27.

---

<sup>12</sup> Айрапетян Н. Творчество в профессии адвоката через призму новых технологий: возможна ли тотальная цифровизация с учетом специфики адвокатской деятельности? // Адвокатская газета. Адвокатская газета [Электронный ресурс]. 27 октября 2022. URL: <https://www.advgazeta.ru/mneniya/tvorchestvo-v-professii-advokata-cherez-prizmu-novykh-tekhnologiy/> (дата обращения: 02.06.2024).

5. Гаврилов С. Н. Об отдельных терминах в области цифровой трансформации адвокатской деятельности и адвокатуры // Адвокатская практика. 2022. № 5. С. 43–50.

6. Гайворонская Я. В., Каримова Ю. И. Цифровизация юридической профессии: о рисках и угрозах цифровизации рынка труда // Advances in law studies. 2020. Т. 8. № 5. С. 55–63.

7. Демиденко Д. Робот-адвокат: как юристам не остаться без работы // Forbes [Электронный ресурс]. 24 апреля 2017. URL: <https://www.forbes.ru/kompanii/343269-robot-advokat-kak-yuristam-ne-ostatsya-bez-raboty> (дата обращения: 12.05.2024).

8. Мрастьева О. С., Семикина С. А. К вопросу о развитии цифровизации и ее влиянии на адвокатуру // Адвокатская практика. 2023. № 3. С. 2–6.

9. Савенко Н. Е. Legaltech в цифровой экономике и правовом регулировании экономической деятельности граждан // Право. Журнал Высшей школы экономики. 2023. Т. 16. № 1. С. 145–171.

10. Согомонян А. Юрист будущего: заучивать законы и кодексы больше нет нужды? // ИПС «Гарант.ру» [Электронный ресурс]. 15 ноября 2017. URL: <https://www.garant.ru/article/1148675/> (дата обращения: 02.06.2024).

**Ekaterina G. Arefinkina**

PhD (in Law), docent,

head of the Criminal Law and Process Department,

Sochi Institute (branch) of the Russian University of Peoples' Friendship  
named after Patrice Lumumba

(Sochi, Russia)

arefinkina@mail.ru

## **DIGITALISATION OF THE ADVOCACY: A NECESSITY OR AN INEVITABILITY?**

**Abstract:** The article examines the process of digitalization of the legal profession in modern society. The authors highlight the main innovations in the activities of the legal profession as a result of the introduction of electronic technologies. The authors consider and analyze both the positive and negative sides of the digitalization of the bar, the system of the Integrated Information System of the Bar of Russia. The article notes that digitalization is aimed at simplified interaction between the court and the lawyer, affects the professional interaction of the lawyer with the principal, where the new «competencies» and capabilities of the lawyer will allow you to track information about the progress of the case, get acquainted with judicial acts. The digitalisation of the advocacy will not be able to work actively without the interaction and digitalisation of the judicial system itself.

**Key words:** advocacy, digitalization, legal proceedings, attorneyclient privilege, chamber of advocates.

**Бахтеев Дмитрий Валерьевич**

Доктор юридических наук, доцент, профессор кафедры криминалистики,  
Уральский государственный юридический университет имени В. Ф. Яковлева  
(г. Екатеринбург, Российская Федерация)  
ae@crimlib.info.

## **ВЕКТОРЫ ЦИФРОВОГО РАЗВИТИЯ КРИМИНАЛИСТИКИ\***

**Аннотация:** работа посвящена обзору двух основных направлений цифровизации в криминалистике: фундаментальному (теоретическому) и функциональному (прикладному). В рамках первого указывается на рассогласование «цифровой криминалистики» с позиций юриспруденции и наук компьютерно-технического профиля. В части второго направления обозреваются основные каналы проникновения технологий в следственную практику, в рамках которых упрощаются рутинные процедуры, повышается эффективность отдельных направлений деятельности или модернизируются способы получения криминалистически значимой информации. Автор приходит к выводу, что в дальнейшем темпы взаимопроникновения криминалистики и компьютерно-технических наук будут только возрастать, что уже сегодня ставит перед профессиональным сообществом задачу модернизировать учебные планы на юридических направлениях подготовки.

**Ключевые слова:** цифровая криминалистика, форензика, цифровые компетенции, цифровизация следственной деятельности, OSINT, дрон, транскрайбер.

Цифровизация как естественный аспект соединения достижений научно-технического прогресса и общественного развития затрагивает большинство сфер человеческой жизни, не исключая и криминалистику. В данной области она может рассматриваться с нескольких позиций.

Во-первых, следует отметить *существование концепции цифровой криминалистики*<sup>1</sup>, которая в настоящее время продолжает вызывать научную дискуссию с позиций как её структуры, содержания, так и места в современной науке. Несмотря на наличие большого числа юридических работ по этой теме, в том числе учебного<sup>2</sup> и монографического характера<sup>3</sup>, необходимо указать, что термин «цифровая криминалистика» уже зарезервирован представителями

---

\* Исследование выполнено за счет гранта Российского научного фонда № 23-78-10011, <https://rscf.ru/project/23-78-10011/>.

<sup>1</sup> В настоящей статье мы не будем вдаваться в дискуссию о корректности этого термина с позиций современной науки.

<sup>2</sup> Цифровая криминалистика: учебник / В. Б. Вехов, С. В. Зуев, Д. В. Бахтеев [и др.]. 2-е издание, дополненное и переработанное. М.: Издательство Юрайт, 2024. 490 с.

<sup>3</sup> Смушкин А. Б. Концепция дистанционной криминалистики. М.: Издательский дом «Юрлитинформ», 2024. 256 с.

технического знания, в котором под ним понимается совокупность технических (а не криминалистических) методов исследования цифровых следов. Система этих методов к настоящему времени не интегрирована в криминалистику и, более того, не имеет устоявшейся собственной структуры.

Полагаем, что в будущем возможны два варианта развития этой концепции.

1. Криминалистическое и техническое знание будут интегрированы, что потребует существенной трансформации компетенций как учёных-криминалистов, так и субъектов расследования преступлений, вплоть до исключения отдельных блоков методов из структуры специальных знаний в пользу знания юридического. В этом же случае терминология будет также стремиться к интеграции и, вероятнее всего, привычные сегодня термины изменят своё понятийное наполнение.

2. Продолжится параллельное развитие юридической (криминалистической) цифровой криминалистики и технической цифровой криминалистики (форензики). В этой модели весьма вероятны появление омонимичных терминов, несовпадение задач и методов их решений.

Указанную дихотомию можно свести к вопросу, поднятому А. М. Кустовым: являются ли цифровые технологии частью криминалистики или криминалистика лишь использует их<sup>4</sup>. К настоящему времени, думается, корректна вторая точка зрения, но, как уже указывалось ранее, ситуация может измениться, хотя это и потребует значительных ресурсов.

Другой аспект цифровизации касается *функционального подхода*, который может рассматриваться в общем или частном проявлении.

Общие функциональные проявления цифровизации относятся к формату использования того или иного технологического решения в процессе раскрытия и расследования преступлений. Обобщённо последствия указанного процесса можно представить в виде следующих явлений.

1. Упрощение существующих подходов. В рамках данного направления привычные для следователя или иного субъекта раскрытия и расследования преступлений действия меняют свой характер и становятся более простыми в реализации или доступными более широкому числу субъектов. Здесь речь может идти об использовании программ-транскрайберов вместо рукописного ведения записей или даже о ставшем уже привычным sms-информировании, постепенно вытесняющим бумажные повестки как способ вызова для участия в производстве следственного действия, судебном заседании.

2. Повышение эффективности отдельных направлений деятельности. Так, использование дронов при осмотре места происшествия, к примеру, при расследовании падения человека с большой высоты, продемонстрировало

---

<sup>4</sup> Кустов А. М. «Цифровая криминалистика» или «цифровые технологии в криминалистике» // Современные технологии и подходы в юридической науке и образовании: Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. С. 173–181.

преимущество этого решения перед съёмкой с подъёмников, вертолётов, соседних зданий<sup>5</sup> и т. п.

3. Формирование новых подходов к получению доказательственной и ориентирующей информации. Так, для сбора сведений о личности и поведении интересующих следствие лиц используются OSINT-технологии<sup>6</sup>, использование дронов вернуло в криминалистическую деятельность обновлённую технологию фотограмметрии, появляются новые технологии 3d- и стереосъёмки.

Вместе с тем, бурный темп цифровизации формирует и новые риски для криминалистики. К таковым можно отнести, в первую очередь, состязательные атаки – формы противодействия расследованию преступлений, непосредственно зависящие от применяемых в расследовании цифровых технологий. Так, лицо, знающее о существовании и возможностях OSINT-методов, может постоянно поддерживать цифрового двойника, демонстрирующего иное поведение в сети и формирующего большое количество нерелевантных для следователя или оперативного сотрудника цифровых следов.

Кроме этого, можно указать на уже существующее расслоение профессионального сообщества в среде как практиков, так и учёных. Если даже уровень общей компьютерной грамотности является неоднородным, то навыки использования цифровых технологий криминалистической направленности встречаются у крайне низкого числа лиц, имеющих отношение к криминалистической деятельности. Полностью поддерживаю мнение Е. Р. Россинской и Т. А. Саакова о насущной необходимости формирования новых инновационных профессиональных компетенций в области IT-технологий<sup>7</sup>. Предполагаем, эта задача не может быть реализована за счёт отдельных спецкурсов в вузах и коротких программ повышения квалификации. Если цифровизация является общим для всех сфер человеческой жизни явлением, программы криминалистической подготовки также должны претерпеть существенные изменения.

Подводя итог всему сказанному выше, подчеркнём очевидную на сегодняшний день мысль: цифровизация – объективная реальность, которая с

---

<sup>5</sup> Севастьянов П. В., Полов В. И., Ивашкова А. В., Томчик С. В. К вопросу о практических аспектах применения беспилотных воздушных судов при проведении осмотра места происшествия // Судебная экспертиза и исследования. 2022. № 1. С. 132–137; Бахтеев Д. В. Тактика использования дронов при осмотре места происшествия // Технологии XXI века в юриспруденции: Материалы четвёртой международной научно-практической конференции, Екатеринбург, 20 мая 2022 года / Отв. редактор: Д. В. Бахтеев. Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2022. С. 47–51.

<sup>6</sup> Бессонов А. А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) // Актуальные вопросы теории и практики оперативно-разыскной деятельности: Сборник научных трудов Межведомственной научно-практической конференции, Москва, 16 сентября 2022 года. М.: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2022. С. 40–45.

<sup>7</sup> Россинская Е. Р., Сааков Т. А. Вектор развития профессиональных компетенций следователя в русле глобальной цифровизации // Уголовный процесс и криминалистика: теория, практика, дидактика: Сборник материалов VII Всероссийской научно-практической конференции, Рязань, 16 декабря 2021 года. Рязань: Академия права и управления Федеральной службы исполнения наказаний, 2022. С. 287–293.

каждым годом всё глубже проникает во все привычные процессы жизнедеятельности. Именно поэтому важно оперативно и, в то же время, научно обоснованно внедрять новые технологии в профессиональную деятельность по раскрытию и расследованию преступлений, интегрировать традиционное гуманитарное знание со специальным компьютерно-техническим и добиваться того, чтобы юристы, особенно субъекты криминалистической деятельности, обладали высоким уровнем цифровых компетенций.

### Список литературы:

1. Бахтеев Д. В. Тактика использования дронов при осмотре места происшествия // Технологии XXI века в юриспруденции: Материалы четвёртой международной научно-практической конференции, Екатеринбург, 20 мая 2022 года / Отв. редактор: Д.В. Бахтеев. Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2022. С. 47–51.

2. Бессонов А. А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) // Актуальные вопросы теории и практики оперативно-разыскной деятельности: Сборник научных трудов Межведомственной научно-практической конференции, Москва, 16 сентября 2022 года. М.: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2022. С. 40–45.

3. Кустов А. М. «Цифровая криминалистика» или «цифровые технологии в криминалистике» // Современные технологии и подходы в юридической науке и образовании: Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. С. 173–181.

4. Россинская Е. Р., Сааков Т. А. Вектор развития профессиональных компетенций следователя в русле глобальной цифровизации // Уголовный процесс и криминалистика: теория, практика, дидактика: Сборник материалов VII Всероссийской научно-практической конференции, Рязань, 16 декабря 2021 года. Рязань: Академия права и управления Федеральной службы исполнения наказаний, 2022. С. 287–293.

5. Севастьянов П. В., Полов В. И., Ивашкова А. В., Томчик С. В. К вопросу о практических аспектах применения беспилотных воздушных судов при проведении осмотра места происшествия // Судебная экспертиза и исследования. 2022. № 1. С. 132–137.

6. Смушкин А. Б. Концепция дистанционной криминалистики. М.: Издательский дом «Юрлитинформ», 2024. 256 с.

7. Цифровая криминалистика: учебник / В. Б. Вехов, С. В. Зуев, Д. В. Бахтеев [и др.]. 2-е издание, дополненное и переработанное. М.: Издательство Юрайт, 2024. 490 с.



**Dmitry V. Bakhteev**

Doctor of Law, Associate Professor, Professor of the Department of Criminalistic,  
Ural State Law University named after V. F. Yakovlev  
(Yekaterinburg, Russian Federation)  
ae@crimlib.info

## **VECTORS OF DIGITAL DEVELOPMENT OF CRIMINALISTIC**

**Abstract:** The paper is devoted to the review of two main directions of digitalization in criminalistic: fundamental (theoretical) and functional (applied). The first one points out the discrepancy of «digital criminalistic» from the positions of jurisprudence and computer science. In part of the second direction, the main channels of technology penetration into investigative practice are reviewed, in which routine procedures are simplified, the efficiency of certain areas of activity is increased, or the methods of obtaining forensically significant information are modernized. The author concludes that in the future the rate of interpenetration of criminalistics and computer and technology science will only increase, which already today poses a challenge to the professional community to modernize curricula in legal training areas.

**Keywords:** digital criminalistic, forensics, digital competencies, digitalization of investigative activities, OSINT, drone, transcriber.

**Бекузарова Юлия Владимировна**

Кандидат юридических наук, доцент кафедры гражданского права,  
Саратовская государственная юридическая академия  
(г. Саратов, Российская Федерация)

## **ВЫСОКОАВТОМАТИЗИРОВАННЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА: ОСНОВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ**

**Аннотация:** В гражданском кодексе не закреплено понятия искусственного интеллекта (ИИ), что вызывает дискуссии относительно отнесения его к объектам либо же к субъектам гражданского права. Несмотря на большое количество теорий правосубъективности ИИ, самой реальной в настоящее время является признание ИИ объектом гражданского права. Сферы применения ИИ очень широки, так беспилотные транспортные средства также наделены технологиями ИИ. Правовое регулирование указанной сферы жизнедеятельности находится на этапе разработки. Так, закреплено определение «высокоавтоматизированных транспортных средств», но главной проблемой остаётся отсутствие специализированного федерального закона. Проект федерального закона, внесённого Министерством транспорта имеет существенные недостатки и находится на этапе доработки. Автор обращает внимание на необходимость проработки вопросов относительно ответственности за вред, причинённый ВАТС, определить круг субъектов, на которых может быть возложена ответственность за причинение вреда, разграничить сферы ответственности указанных субъектов.

**Ключевые слова:** высокоавтоматизированные транспортные средства, беспилотный автомобиль, возмещение вреда, деликтное право, искусственный интеллект.

Отсутствие в нормах Гражданского кодекса РФ понятия искусственный интеллект приводит к дискуссии в вопросах отнесения его либо к объектам гражданских правоотношений, либо к их субъектам. На сегодняшний день существуют различные концепции правосубъектности искусственного интеллекта. Одни авторы считают, что существует необходимость отнесения ИИ к субъектам гражданского права, наряду с физическими и юридическими лицами, другие, не соглашаясь с данной точкой зрения, высказывают свою, обосновывая необходимость рассматривать ИИ в качестве объектов гражданского права. Основой данной теории является отсутствие у искусственного интеллекта признаков субъекта права, которые присущи человеку: сознания, чувств, воли и т. д. Однако представители указанной концепции не учитывают автономность искусственного интеллекта и его способность принимать самостоятельные решения, что, в свою очередь, свидетельствует о недостатках данной позиции.

Другие исследователи, учитывающие признак автономности систем искусственного интеллекта, предлагают распространить на них режим, применяемый к животным<sup>1</sup>.

Другие авторы предлагают искусственный интеллект наделить статусом юридического лица<sup>2</sup>.

Несмотря на наличие множества теорий правосубъектности ИИ, технологический прогресс идёт вперёд и уже не осталось такой сферы жизнедеятельности человека, где бы не использовался ИИ. Искусственный интеллект нашёл широкое применение в областях медицины, финансов, промышленности, образования, транспорта, сельского хозяйства и др.

Также искусственным интеллектом наделены и беспилотные транспортные средства. На территории России компании «Яндекс»<sup>3</sup>, «КАМАЗ»<sup>4</sup> и Горьковский автомобильный завод представили беспилотные транспортные средства<sup>5</sup>.

В законодательстве закреплена дефиниция таких транспортных средств. Так в Постановлении правительства от 17.10.22 г. № 1849 говорится о «высокоавтоматизированном транспортном средстве, которое сертифицировано в установленном законодательством РФ порядке и оснащено автоматизированной системой вождения, предназначенное в том числе и для перевозки грузов (далее ВАТС)»<sup>6</sup>. Уровень автоматизации ВАТС зависит от уровня используемого ИИ.

Главной проблемой правового регулирования беспилотных транспортных средств остаётся отсутствие специального Федерального закона. Министерством транспорта РФ в 2021 г. был подготовлен проект Федерального закона «О высокоавтоматизированных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации»<sup>7</sup>. Однако он содержит

---

<sup>1</sup> Дремлюга Р. И., Дремлюга О. А. Искусственный интеллект – субъект права: аргументы за и против // Правовая политика и правовая жизнь. 2019. № 2. С. 123.

<sup>2</sup> Незнамов А. В., Наумов В. Б. Стратегия регулирования робототехники и киберфизических систем // Закон. 2018. № 2. С. 81.

<sup>3</sup> «Яндекс» построил беспилотник на базе гибридной Toyota // Коммерсантъ [Электронный ресурс]. 31 мая 2017 г. URL: <https://www.kommersant.ru/doc/3312874?ysclid=la6ne1wqpi549970866> (дата обращения: 13.05.2024).

<sup>4</sup> «КАМАЗ» на форуме Kazan Digital Week-2022 // KAMAZ [Электронный ресурс]. 21 сентября 2022 г. URL: [https://kamaz.ru/press/releases/kamaz\\_na\\_forume\\_kazan\\_digital\\_week\\_2022/](https://kamaz.ru/press/releases/kamaz_na_forume_kazan_digital_week_2022/) (дата обращения: 13.05.2024).

<sup>5</sup> ГАЗ представил опытные образцы беспилотных автомобилей // АвтоцентрГАЗ лидер [Электронный ресурс]. 29 августа 2018 г. URL: <https://gazlider.ru/about-company/news/gaz-predstavil-opitnie-obraztsi-bespilotnih-avtomobilei/> (дата обращения: 13.05.2024).

<sup>6</sup> Постановление Правительства РФ от 17.10.2022 № 1849 (ред. от 14.02.2024) «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств в отношении реализации инициативы «Беспилотные логистические коридоры» на автомобильной дороге общего пользования федерального значения М-11 «Нева» // Собрание законодательства РФ. 2022. № 43. Ст. 7409.

<sup>7</sup> Проект Федерального закона «О высокоавтоматизированных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации» (подготовлен Минтрансом России) (не внесен в ГД ФС РФ, текст по состоянию на 19.05.2022) // СПС «КонсультантПлюс»

ряд недостатков, одним из которых является положение о деликтной ответственности в случае причинения вреда ВАТС. В Законопроекте предусмотрена одна норма, которая носит отсылочный характер к нормам ГК РФ.

Исходя из легального определения ВАТС, видно, что законодатель относит его к транспортным средствам. Таким образом, можно сделать вывод, что ВАТС также, как и транспортные средства в рамках гражданского законодательства, относятся к источникам повышенной опасности в вопросах ответственности за причинённый вред.

Согласно положению статьи 1079 ГК РФ вред, причинённый источником повышенной опасности, возмещает владелец такого источника (собственник, арендатор, поверенный на основании доверенности). Но в данном случае стоит учитывать специфику регулируемых правоотношений и особенности самого источника повышенной опасности. ВАТС не просто автотранспортное средство, а оснащённое программным обеспечением на основе искусственного интеллекта, которое способно самостоятельно передвигаться в пространстве без посторонней помощи. К тому же, называя владельцев ВАТС в качестве субъектов ответственности, мы сознательно вычёркиваем из этого круга других участников данных правоотношений, к которым в первую очередь относится изготовитель ВАТС. Видится целесообразным внести в законопроект «О высокоавтоматизированных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации» специальную норму об ответственности производителя ВАТС.

Возникает вопрос о соотношении ответственности между производителем и владельцем ВАТС. Так как главной функцией гражданской ответственности является компенсаторная, направленная на компенсацию ущерба, причинённого правонарушением, то наилучшим образом этому будет способствовать установление солидарной ответственности производителя и владельца ВАТС. Солидарная ответственность в соответствии со статьёй 323 ГК РФ позволит уполномоченным лицам требовать возмещения причинённого им вреда от каждого из причинителей в отдельности как в части долга, так и в полном объёме, а также одновременно от всех причинителей вреда.

В обоснование выбора именно солидарной ответственности для владельцев и производителей ВАТС можно также обратиться к статье 134 ГК РФ: транспортное средство и искусственный интеллект, позволяющий самостоятельно передвигаться в пространстве, соединены и взаимосвязаны настолько, что предполагают их использование по общему назначению, распространяя на них режим сложной вещи.

К тому же привлечение к ответственности производителя ВАТС можно обосновать наличием статьи 1095 ГК, где предусмотрено, что вред, причинённый жизни, здоровью или имуществу гражданина либо имуществу

юридического лица вследствие конструктивных, рецептурных или иных недостатков товара, работы или услуги, а также вследствие недостоверной или недостаточной информации о товаре (работе, услуге), подлежит возмещению продавцом или изготовителем товара, лицом, выполнившим работу или оказавшим услугу (исполнителем), независимо от их вины и от того, состоял потерпевший с ними в договорных отношениях или нет.

Таким образом вышеуказанный законопроект нуждается в дальнейшей доработке его положений. Необходимо сделать отсылку к статье 1079 ГК РФ, предусматривающей ответственность за вред, причинённый источником повышенной опасности. Также необходимо разграничить ВАС по степени опасности. То есть решить вопрос относительно того, все ли ВАС будут приравниваться к источникам повышенной опасности или же нет, и выделить признаки, по которым возможно провести разграничение. Целесообразно решить вопрос о разграничении сфер ответственности субъектов указанных правоотношений, определить вид ответственности изготовителя и владельца ВАС.

### **Список литературы**

1. Дремлюга Р. И., Дремлюга О. А. Искусственный интеллект – субъект права: аргументы за и против // Правовая политика и правовая жизнь. 2019. № 2. С. 120–125.
2. Незнамов А. В., Наумов В. Б. Стратегия регулирования робототехники и киберфизических систем // Закон. 2018. № 2. С. 69–89.

**Yuliay V. Bekuzarova**

PhD (Law), Associate Professor of the Department of Civil Law,  
Saratov State Law Academy  
(Saratov, Russian Federation)

### **ARTIFICIAL INTELLIGENCE AND HIGHLY AUTOMATED VEHICLES: FUNDAMENTALS OF LEGAL REGULATION**

**Abstract:** The concept of artificial intelligence is not fixed in the Civil Code, which causes discussions regarding its attribution to objects or subjects of civil law. Despite the large number of theories of legal subjectivity of AI, the most real one at present is the recognition of AI as an object of civil law. The scope of AI applications is very wide, as unmanned vehicles are also endowed with AI technologies. The legal regulation of this sphere of life is at the stage of development. Thus, the definition of «highly automated vehicles» has been fixed, but the main problem remains the lack of a specialized federal law. The draft federal law introduced by the Ministry of Transport has significant drawbacks and is at the stage of completion. The author draws attention to the need to work out issues regarding liability for damage caused by VATS. To

determine the range of subjects who may be held responsible for causing harm, to delineate the areas of responsibility of these subjects.

**Keywords:** highly automated vehicles, self-driving car, compensation for harm, tort law, artificial intelligence.

**Блинов Александр Георгиевич**

Доктор юридических наук, заведующий кафедрой уголовного и  
уголовно-исполнительного права,  
Саратовская государственная юридическая академия  
(г. Саратов, Российская Федерация)  
blinovag2008@yandex.ru

**Герасимов Александр Михайлович**

Доктор юридических наук, профессор кафедры уголовного и  
уголовно-исполнительного права,  
Саратовская государственная юридическая академия  
(г. Саратов, Российская Федерация)  
amgerasimov@list.ru

## **УГОЛОВНО-ПРАВОВАЯ ОХРАНА ГЕНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ ЧЕЛОВЕЧЕСТВА В РОССИИ**

**Аннотация:** Исследование ориентировано на обоснование рисков направленного редактирования генома эмбриона человека, предопределяющих развитие теории уголовно-правового обеспечения в России генетической безопасности человечества. Его цель заключается в формировании модели умеренного правового воздействия на сознание и волю учёного-экспериментатора инструментами уголовного законодательства, отвечающей потребностям современного общества и интересам инновационной науки. Методологию обеспечения поставленной цели составили диалектический метод как универсальный инструмент познания в сочетании с методикой догматического (формально-юридического) анализа, дискурс-анализа и ситуационного анализа (case study). Результатом исследования стало обоснование идеи, согласно которой правовое сопровождение анализируемой сферы в отечественном правовом пространстве рационально выстраивать с акцентом на диспозитивные ресурсы регулятивных отраслей законодательства. Уголовному праву, оперирующему методом императивным, должна быть отведена роль инструмента, оказывающего стимулирующее воздействие на поведение исследователей, которые демонстрируют готовность пренебрегать генетической безопасностью человечества ради удовлетворения собственных амбиций. По итогам исследования сделан вывод о необходимости разработать уголовно-правовую норму, способную обеспечивать генетическую безопасность людей в России.

**Ключевые слова:** генетическая безопасность, редактирование генома, правовое регулирование, юридическая охрана, уголовное право.

Глобальные достижения генетических исследований, некоторое время назад воспринимавшиеся в качестве научных сенсаций, сегодня активно внедряются в медицинскую практику. Арсенал превентивной медицины пополнен методиками генетического скрининга, позволяющими пациенту уточнить существующие диагнозы и выявить риски развития в будущем моногенных и многофакторных заболеваний. В их числе новообразования, муковисцидоз, фенилкетонурия, нарушения свёртываемости крови, гемофилия, кистозный фиброз и многие другие. Фармакологическая отрасль обогатилась новым классом лекарственных препаратов, созданных на основе РНК-интерференции. Они дают шанс пациентам на исцеление от таких редких наследственных заболеваний как семейная амилоидная полиневропатия и острая печёночная порфирия. В то же время научное сообщество практически единодушно сходится во мнении, что наиболее внушительные резервы биомедицины заложены в методиках направленного изменения генома. Среди них лидирует технология CRISPR/Cas9, дающая возможность практически с ювелирной точностью редактировать геном человека. По оценкам специалистов, в обозримом будущем генетический редактор позволит освободить от нежелательных последствий потомственного копирования целые поколения.

Между тем за впечатляющими перспективами применения инновационной биотехнологии скрывается чрезвычайно важная социальная проблема. На сегодняшний день наука не в состоянии просчитать все потенциальные последствия редактирования генома людей. Изменяя один или несколько из трёх миллиардов нуклеотидов, образующих геном человека, невозможно абсолютно точно смоделировать реакцию иных генов наследственного механизма. Негативное фоновое явление, вызываемое использованием генных редакторов, получило наименование «Off target effects» и предполагает возникновение нецелевых генетических модификаций. Подобный удар вне генетической мишени чреват непредсказуемыми результатами эксперимента. Эмбрион с отредактированным геномом рискует быть нежизнеспособным и погибнуть внутриутробно. У новорождённого ребёнка, генетический код которого скорректирован с целью купирования одного тяжелого заболевания, вполне может быть сформирована предрасположенность к другим недугам<sup>1</sup>.

Особую остроту ситуации придаёт вероятность мутагенной цепной реакции, грозящей распространением нежелательной генетической мутации в популяции людей. В правовых аспектах речь идёт о нарушении генетической безопасности, под которой следует понимать «защищенность генетической информации Homo sapiens от неправомерного воздействия физических лиц, причиняющих вред либо создающих угрозу его причинения»<sup>2</sup>.

---

<sup>1</sup> См.: Costas J. The highly pleiotropic gene SLC39A8 as an opportunity to gain insight into the molecular pathogenesis of schizophrenia // Am. J. Med. Genet. 2018. P. 274–283.

<sup>2</sup> Блинов А. Г. Генетическая безопасность Homo sapiens и модель ее уголовно-правового обеспечения // Развитие наук антикриминального цикла в свете глобальных вызовов обществу: сборник трудов по материалам всероссийской заочной научно-практической конференции с международным участием (Саратов, 16 октября 2020 г.) / под общ. ред. А. Г. Блинова, Е. В. Кобзевой. Саратов, 2021. С. 11.



Социальной и правовой практике известны неконтролируемые клинические эксперименты, связанные с наследуемыми изменениями ДНК отдельного человека, угрожающие генетической безопасности всего человечества. Как известно, первый подобный эксперимент в 2018 г. провела группа китайских учёных под руководством Хэ Цзянькуя. Относительно результатов его деятельности свою озабоченность выразили учёные из всего мира. Особенно показательно, что ввести глобальный мораторий на все клинические эксперименты по редактированию наследственной программы человека потребовали одни из создателей технологии CRISPR/Cas Ф. Чжан, Э. Шарпентье и их коллеги из семи стран. С точки зрения учёных, ни один генетический эксперимент не должен проводиться без установления его долгосрочных биологических последствий не только для конкретного пациента, но для всего человеческого вида<sup>3</sup>.

Здравый смысл в обозначенных призывах авторитетных исследователей присутствует. Как показывает практика, стремление занять лидирующие позиции в инновационном секторе биомедицины побуждает некоторых учёных к возвышению своих исследовательских амбиций над интересами науки. В таких случаях допустимый профессиональный риск перестаёт быть обоснованным. Опережение разумных сроков клинических испытаний по редактированию генома *Homo sapiens* в разы увеличивает вероятность возникновения фатальных последствий для человечества.

Научное сообщество вполне обоснованно обращает внимание на потребность тщательной независимой научной оценки результатов исследовательских проектов, предполагающих вмешательство в наследственную программу людей. Однако соответствующие требования не могут ограничиваться рамками профессиональной этики и должны обрести легитимную форму. На государственном уровне своего разрешения ожидают юридически значимые вопросы, касающиеся допустимых границ доклинических и клинических экспериментов с ДНК человека, а также ответственности за нарушения установленных нормативных предписаний.

Однако в области инновационной медицины недопустимы радикальные правовые решения, устанавливающие полный запрет на применение технологий направленного изменения генома человека. Они могут спровоцировать социальные проблемы, связанные искусственным замедлением развития отечественных генетических исследований и создаваемых на их основе биотехнологий. Запрет на применение генетических редакторов лишит огромное количество людей надежды на избавление от тяжёлых заболеваний, многие десятилетия передаваемых от поколения к поколению.

Отечественному законодателю рекомендуется сконцентрировать основные усилия на формировании правовой основы проведения исследований по редактированию генома эмбриона человека. Правовое обеспечение генетической безопасности человечества логично выстраивать на принципах

---

<sup>3</sup> Lander E., Baylis F., Zhang F., Charpentier E., Berg P. [et al]. Adopt a moratorium on heritable genome editing // Nature. 2019. Vol. 567. P. 165–168.

приоритетной реализации альтернативных методов предупреждения наследственных аномалий, а также необходимой апробации и получения независимых положительных экспертных оценок внедряемых в медицинскую практику биотехнологий. При этом надлежащее правовое регулирование инновационной медицинской деятельности высвечивает границы объекта, нуждающегося в охране. На сегодняшний день востребована уголовно-правовая норма, запрещающая под угрозой наказания незаконное клиническое исследование, направленное на редактирование генома эмбриона человека в репродуктивных целях.

Совершенно очевидно, что наибольшее внимание проблеме безопасности человечества в ходе клинических испытаний технологий направленного изменения генома должны уделять страны, располагающие соответствующими научными знаниями, методиками и оборудованием. К их числу небезосновательно относится Российская Федерация, представители научного сообщества которой демонстрируют заметные успехи в редактировании человеческого генома. В подтверждение сказанного достаточно сослаться на результаты работы группы отечественных исследователей под руководством Д. В. Ребрикова, доказывающая эффективность технологии CRISPR/Cas9. По результатам проведённых опытов с аномальными человеческими зиготами, полученными от 11 супружеских пар, учёные пришли к выводу о том, что «изменение гена CCR5 путем редактирования генома CD4<sup>+</sup>-Т-клеток является одним из способов предотвращения распространения ВИЧ-1-инфекции. Однако похожая стратегия защиты от ВИЧ может быть использована и для защиты плода ВИЧ-инфицированных женщин со слабым ответом на антиретровирусную терапию. Создание «естественного» аллеля CCR5delta32 на стадии зиготы может защитить плод от ВИЧ-инфекции во время внутриутробного развития и родов»<sup>4</sup>. Д. В. Ребриков неоднократно высказывался относительно необходимости информативности методик оценки безопасности технологии CRISPR/Cas9, что предопределяет её возможность применения в клинической практике.

Как и многим странам мира, Российской Федерации только предстоит сформировать механизм юридического обеспечения соответствующих исследований. На сегодняшний день отечественное правовое пространство располагает скромным количеством документов, упорядочивающих некоторые аспекты генно-инженерной деятельности и использования её результатов в жизнедеятельности людей, проведения государственной геномной регистрации, вводящих временный запрет на клонирование человека, определяющих оборот биомедицинских клеточных продуктов. Однако правовые параметры экспериментов по редактированию генома человека на сегодняшний день не определены. Инновационная биомедицина, по существу, остаётся саморегулируемым сектором системы здравоохранения.

---

<sup>4</sup> Кодылева Т. А., Кириллова А. О., Тыщик Е. А., Макаров В. В., Хромов А. В., Гушин В. А., Абубакиров А. Н., Ребриков Д. В., Сухих Г. Т. Эффективность создания делеции CCR5Ddelta32 методом CRISPR-Cas9 в эмбрионах человека // Вестник Российского государственного медицинского университета. 2018. № 4. С. 80.

Одновременно потребуется охрана формируемых отношений в рассматриваемом секторе биомедицины. В отечественном правовом пространстве к разряду охранительных отраслей права относятся административно-деликтное и уголовное законодательство. Ресурс законодательства об административных правонарушениях задействуется в том случае, когда вред от оцениваемого деяния ограничивается нарушением правового порядка. Отрасль ориентирована на удержание человека от деяний, оказывающих отрицательное воздействие не на сущностные свойства социально значимых связей, а на их юридическую оболочку. В рассматриваемых аспектах необходимо отметить, что на сегодняшний день административно-деликтное право располагает нормой, устанавливающей ответственность за нарушение законодательства Российской Федерации в области генно-инженерной деятельности (ст. 6.3.1. КоАП РФ).

В ситуациях, когда совокупный вред от оцениваемого деяния существенным образом затрагивает фактические интересы личности, общества, государства и тем самым угрожает сложившемуся в обществе материальному порядку, возникает потребность в активации уголовного законодательства. Его цель заключается в удержании неустойчивых лиц от совершения деяний, достигающих уровня общественной опасности. В рамках проводимого исследования небезынтересно, что долгое время уголовное право напрямую не вмешивалось в область инновационной медицины. Между тем стремительное развитие биомедицинских технологий обуславливает объективно выраженную потребность в уголовно-правовом удержании претензионных исследователей от проведения незаконных экспериментов по наследуемому изменению генома эмбриона человека. Располагая необходимым принудительным механизмом, уголовное право в состоянии нивелировать «нездоровую» мотивацию учёных-экспериментаторов. Конкретная модель уголовно-правовой нормы, ориентированной на охрану генетической безопасности нами предлагалась в предыдущих исследованиях<sup>5</sup>.

### Список литературы

1. Блинов А. Г., Герасимов А. М. Теоретическая модель преступных деяний в сфере исследования генома человека // Вестник Омского университета. Серия «Право». 2020. Т. 17. № 2. С. 76–85.
2. Блинов А. Г. Генетическая безопасность Homo sapiens и модель ее уголовно-правового обеспечения // Развитие наук антикриминального цикла в свете глобальных вызовов обществу: сборник трудов по материалам всероссийской заочной научно-практической конференции с международным участием (Саратов, 16 октября 2020 г.) / под общ. ред. А. Г. Блинова, Е. В. Кобзевой; ФГБОУ ВО «Саратовская государственная юридическая академия».

---

<sup>5</sup> Блинов А. Г., Герасимов А. М. Теоретическая модель преступных деяний в сфере исследования генома человека // Вестник Омского университета. Серия «Право». 2020. Т. 17. № 2. С. 76–85.

Саратов: Изд-во ФГБОУ ВО «Саратовская государственная юридическая академия», 2021. С. 6–15.

3. Кодылева Т. А., Кириллова А. О., Тыщик Е. А., Макаров В. В., Хромов А. В., Гущин В. А., Абубакиров А. Н., Ребриков Д. В., Сухих Г. Т. Эффективность создания делеции CCR5Ddelta32 методом CRISPR-Cas9 в эмбрионах человека // Вестник Российского государственного медицинского университета. 2018. № 4. С. 80–84.

4. Costas J. The highly pleiotropic gene SLC39A8 as an opportunity to gain insight into the molecular pathogenesis of schizophrenia // Am. J. Med. Genet. 2018. P. 274–283.

5. Lander E., Baylis F., Zhang F., Charpentier E., Berg P. [et al]. Adopt a moratorium on heritable genome editing // Nature. 2019. Vol. 567. P. 165–168.

**Blinov Alexander Georgievich**

Doctor of Law, Head of the Department of Criminal and penal law,  
Saratov State Law Academy  
(Saratov, Russian Federation)  
blinovag2008@yandex.ru

**Gerasimov Alexander Mikhailovich**

Doctor of Law, Professor of the Department of Criminal and Penal Law,  
Saratov State Law Academy  
(Saratov, Russian Federation)  
amgerasimov@list.ru

**CRIMINAL LAW PROTECTION OF GENETIC HUMAN SECURITY IN  
RUSSIA**

**Abstract:** The study is focused on substantiating the risks of directed editing of the human embryo genome, which predetermine the development of the theory of criminal law support in Russia for the genetic safety of mankind. Its purpose is to form a model of moderate legal influence on the consciousness and will of the experimental scientist by means of criminal legislation that meets the needs of modern society and the interests of innovative science. The methodology for ensuring the set goal was the dialectical method as a universal tool of cognition in combination with the methodology of dogmatic (formal-legal) analysis, discourse analysis and situational analysis (case study). The result of the study was the substantiation of the idea that it is rational to build legal support for the analyzed sphere in the domestic legal space with an emphasis on the dispositive resources of regulatory branches of legislation. Criminal law using the imperative method should be given the role of a tool that has a stimulating effect on the behavior of researchers who demonstrate a willingness to neglect the genetic safety of humanity in order to satisfy their own ambitions. According to the results of the study, it was concluded that it is necessary to develop a criminal law that can ensure genetic safety in Russia.

**Keywords:** genetic safety, genome editing, legal regulation, legal protection, criminal law.

**Галяшина Елена Игоревна**

Доктор юридических наук, доктор филологических наук, профессор,  
заведующий кафедрой криминалистики,  
Московский государственный юридический университет  
имени О. Е. Кутафина (МГЮА)  
(г. Москва, Российская Федерация)  
eigaljashina@msal.ru

### **ПЕРЕПИСКА В МЕССЕНДЖЕРАХ КАК ИСТОЧНИК КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ: ОСОБЕННОСТИ СОБИРАНИЯ И ИССЛЕДОВАНИЯ**

**Аннотация:** В статье освещаются возможности получения криминалистически значимой информации по материалам переписки в мессенджерах. Автор обращает внимание на широкий круг объектов, объединяемых собирательным понятием «переписка в мессенджере», к числу которых относятся не только письменные тексты сообщений, но и мультимедийный контент, аудио, видеофайлы, изображения, анимации и т. д., что предопределяет необходимость использования комплекса разносторонних специальных знаний для их собирания и исследования.

**Ключевые слова:** криминалистически значимая информация, переписка, письменный текст, аудиофайлы, видеофайлы, специальные знания.

Технологический прогресс позволил внедрить в повседневное общение мессенджеры – программы, которые предназначены для онлайн-коммуникации – мгновенного обмена текстовыми сообщениями и мультимедиа между пользователями сети Интернет. Использовать программу мессенджер можно на компьютере, смартфоне или планшете – в приложении либо веб-версии для браузера. В зависимости от возможностей конкретной программы, с помощью мессенджера можно общаться с другими пользователями, отправлять текстовые или голосовые сообщения, а также смайлы или эмодзи (анимационные изображения для показа эмоции или действия), стикеры, фото, видео и другие файлы; можно звонить и разговаривать по видеосвязи, в том числе и в режиме видеоконференции. В обиходе вся электронная корреспонденция, отправляемая посредством мессенджера, именуется перепиской, что, конечно, носит условный характер, т. к. современные средства коммуникации намного многообразнее письменных сообщений, традиционно относимых к эпистолярному жанру.

Надо отметить, что социальные сети также, как и мессенджеры, предназначены для межличностного или группового общения. Но их функциональность шире – они сочетают чат, новостную ленту, аудио- и видеостриминг, игровой хостинг, маркетплейс товаров, сервис знакомств и т. д.

У некоторых соцсетей, например, ВКонтакте, есть собственный мессенджер, связанный с платформой, но выделенный в отдельный сервис – «VK Мессенджер», в котором можно общаться с друзьями из социальной сети и людьми, которые сохранены в телефонной книге. Имеется даже расшифровка аудиосообщений с использованием технологии распознавания речи на базе нейросетей, а сами голосовые сообщения можно воспроизводить в ускоренном или замедленном режиме

Некоторые мессенджеры, например Telegram, позволяют создавать каналы и публиковать в них контент для широкой аудитории.

Размещаемая пользователем на своей странице в социальной сети информация при корректном подходе к её поиску, обнаружению и исследованию может быть весьма полезной для криминалистического анализа личности автора, установления иных фактических данных, без которых при расследовании преступлений и судебном рассмотрении конкретных уголовных дел зачастую не могут быть реализованы задачи уголовного судопроизводства<sup>1</sup>.

Для криминалистики может быть важна персональная информация о зарегистрированном пользователе: его фамилия, имя, отчество; дата и место рождения; место жительства и (или) регистрации; место работы; место учёбы; номер телефона. Также можно получить сведения о внешности лица по фотографиям и видеозаписям, имеющимся на странице, об интересах пользователя, социальном окружении, местонахождении и т. д. По фото или видеоизображениям можно определить примерный возраст, рост, комплекцию, пол пользователя, его психофизиологическое состояние. По аватару – графическому представлению пользователя – можно составить представление о его психологических качествах, интересах, увлечениях, каких-либо специфических чертах характера. Аватар позволяет создать определённое впечатление у собеседников о внутреннем духовном мире и статусе пользователя. Этим же целям может служить и никнейм – псевдоним в сетевом, виртуальном пространстве, который самостоятельно присваивается его носителем. И аватар, и никнейм можно рассматривать как результат саморефлексии, отражающий внутренний мир личности, поскольку оба компонента позволяют пользователю представлять себя так, как он хочет: скрыть или показать особенности характера, описать настроение, акцентировать внимание на внешних данных, рассказать о своих предпочтениях. Этой же цели служат статусы, которые устанавливаются почти в любом мессенджере сегодня и могут изменяться намного чаще, чем аватар и никнейм.

В качестве криминалистически значимой информации существенное значение сегодня приобретает переписка между пользователями мессенджера или социальной сети. Это могут текстовые сообщения, фото-, видео- и аудиофайлы, графические и символные материалы. Переписка может содержать как ориентирующую, так и доказательственную информацию об

---

<sup>1</sup> Олиндер Н. В., Гамбарова Е. А. О результатах эксперимента «Поиск и восприятие информации о личности в сети Интернет и ее использование при расследовании преступлений» // Эксперт-криминалист. 2017. № 4. С. 29–31.

обстоятельствах, входящих в предмет доказывания или имеющих вспомогательное значение<sup>2</sup>. Кроме того, такая информация может свидетельствовать о подготовке к совершению преступления, его организации, сокрытии следов и т. п.

Текстовое сообщение может выступать объектом как идентификационного, так и диагностического автороведческого исследования, целью которого является установление социо-биографических данных об авторе<sup>3</sup>. Современная наука полна сведений о наличии корреляционных связей между особенностями реализации в письменном тексте речевой функции человека и его индивидуальными (групповыми) характеристиками<sup>4</sup>. Наиболее устойчивые связи обнаружены с такими характеристиками как пол, возраст, языковая среда, в которой формировалась личность (территориальная, национально-языковая принадлежность, образование, сфера деятельности), темперамент, психопатология и др.

Исследователи отмечают, что «при проведении экспертного анализа признаков речи автора эффективны также методы диагностического исследования в целях определения гендера, возраста, индивидуально-личностных и иных характеристик автора, а также оценки однородности авторских признаков, исключения алгоритмов автоматизированной генерации текстов. Диагностика характеристик автора может выступать как самостоятельная экспертная задача и как этап проведения идентификации. В связи со спецификой переписок в мессенджере представляется актуальным изучение гендерных особенностей языковой личности, проявляющихся в формате быстрого обмена личными сообщениями (выбор языковых и неязыковых средств, обусловленный гендером адресанта и адресата; фактор влияния собеседников на признаки речи друг друга)»<sup>5</sup>.

С точки зрения психологии содержание речевой деятельности в социальной сети не сводится только к использованию средств языка для передачи сообщения. Исходным моментом для речевого общения является мотив высказывания или потребность в передаче сообщения. Затем путём внутреннего программирования общий замысел высказывания в соответствии с имеющимися у автора стереотипами трансформируется в форму предметно-образного языкового кода, который и передаётся посредством письменной или устной речи. В этой связи задача получения криминалистически значимой

---

<sup>2</sup> Клевцов К. К. Переписка в мессенджерах как доказательство. Способы получения и оформления // Уголовный процесс. 2020. № 10. С. 42–45.

<sup>3</sup> Сааков Т. А. Алгоритм судебно-экспертного исследования демографических характеристик автора по признакам письменной речи в эпоху цифровизации // Проблемы правоохранительной деятельности. 2021. № 3. С. 14–22.

<sup>4</sup> Мухин М. Ю., Лозовская А. И. Социальная сеть как источник социолингвистических данных: лексико-статистический анализ // Вестник ЮУрГУ. Серия «Лингвистика». 2019. Т. 16. № 4. С. 38–44.

<sup>5</sup> Громова А. В. Переписка в мессенджере: идентификация автора по тексту в условиях трансформации индивидуализирующих признаков // Вестник Волгоградского государственного университета. Серия 2, Языкознание. 2021. Т. 20. № 2. С. 94–95.



информации по размещённым в социальных сетях материалам встречает ряд сложностей, без учёта которых получение достоверных сведений невозможно<sup>6</sup>.

Во-первых, необходимо учитывать возможность создания фейковых аккаунтов (учётных записей, сформированных от имени других пользователей), на которых размещаются ложные сведения о его владельце как путём внесения сведений о вымышленных персонажах, так и посредством незаконного использования персональных данных реального лица. Фейковые аккаунты могут снабжаться фотографией, персональной информацией об имитируемых пользователях и иными данными<sup>7</sup>.

Во-вторых, текстовые сообщения могут формироваться автором под воздействием естественных сбивающих факторов (в условиях ограниченной видимости или в движении) и/или с маскировкой собственных и/или имитацией чужих письменно-речевых навыков. Под маскировкой понимается намеренное изменение автором текста формально-содержательной (смысловой) и языковой структуры своей письменной речи с целью скрыть информацию о себе или дать заведомо ложную информацию о своей языковой идентичности.

Так, например, исследование переписки в чате пользователя, подозреваемого в совершении преступления в отношении половой неприкосновенности несовершеннолетнего, позволило экспертам-криминалистам обнаружить признаки доминирования гендерно маркированных характеристик, соотносимых с мужским типом речи лица, представлявшегося на своей странице девушкой 19 лет. Стилистика речи автора соответствовала признакам возрастной группы 35–50 лет. Автору текстового сообщения были свойственны следующие индивидуально-личностные характеристики: активность, доминирование, общительность, привлечение внимания, соперничество, демонстративность, предусмотрительность, эмоциональная неустойчивость; игривость (любопытство, артистичность).

Характерные лексические, синтаксические и паралингвистические особенности переписки в мессенджере отражают специфику интернет-коммуникации как устно-письменного дискурса. Коммуникативная ситуация общения в мессенджере представлена разговорным стилем и детерминирована как фактом синхронности, так и технологическими особенностями самого мессенджера<sup>8</sup>.

Существенным фактором является выявление признаков преднамеренных искажений, в том числе умышленной маскировки индивидуальных языковых навыков. Знание о ситуации коммуникации позволяет отличить признаки письменно-речевых навыков, являющихся следствием воздействия на речевую

---

<sup>6</sup> Литвинова Т. А., Бирюкова Е. Д., Загоровская О. В. Диагностирование пола, возраста и психологических характеристик автора письменного текста с использованием методов корпусной и компьютерной лингвистики: возможности и ограничения // Вопросы криминологии, криминалистики и судебной экспертизы. 2021. № 1 (49). С. 105–111.

<sup>7</sup> Кавеева А. Д., Гурин К. Е. Искусственные профили «ВКонтакте» и их влияние на социальную сеть пользователей // Журнал социологии и социальной антропологии. 2018. № 21 (2). С. 214–231.

<sup>8</sup> Горошко Е. И., Землякова Е. А. Полиформатный мессенджер как жанр 2.0 (на примере мессенджера мгновенных сообщений Telegram) // Жанры речи. 2017. № 1 (15). С. 97–100.

деятельность естественных внешних факторов (набор текста на клавиатуре мобильного телефона в движущемся транспорте, в условиях плохой видимости, в состоянии ажитации, сильного психомоторного или эмоционального напряжения, депрессивного психоэмоционального расстройства, алкогольного / наркотического опьянения и т. д.), от намеренного искажения таких навыков.

В-третьих, исключительно большое значение для успешного проведения идентификации автора по признакам его письменной речи в интернет-переписке имеет лингвистическая сопоставимость сравниваемых текстов, обусловленная речевой реализацией в конкретной коммуникативной ситуации. Для категорического вывода о тождестве автора сообщений индивидуализирующие особенности письменной речи должны обладать различительной способностью и идентификационной значимостью, устойчивостью, проявляться в достаточном количестве системно на всех уровнях языка, и в своей совокупности обладать индивидуальностью, достаточной для установления индивидуально-конкретного тождества.

А. В. Громова справедливо подчёркивает, что «исследование материалов переписки в мессенджерах проводится с учётом особенностей выбора автором языковых средств в условиях интернет-коммуникации, а также используемого при создании сообщений интерфейса мессенджера и типа электронного устройства (размер экрана, его состояние, клавиатура и др.)»<sup>9</sup>. Как показывает экспертная практика, индивидуализирующие признаки с различной степенью идентификационной значимости могут проявляться на коммуникативном, графическом и лексико-грамматическом уровнях. На коммуникативном уровне, наибольшей устойчивостью к искажениям, в том числе имитации и маскировке, обладают в числе прочих: предпочитаемые средства выражения субъективной модальности, средства воздействия на адресата, способы актуализации сообщаемого, а также особенности игрового поведения и средств самопрезентации. На графическом уровне – особенности структурирования (парцелляции) текста, особенности использования знаков раскладки клавиатуры, постановки пробелов между словами, использования знаков пунктуации, прописных / строчных букв, смайликов, эмодзи, цифр и иных иконических символов. На лексико-грамматическом уровне – предпочтение в выборе вариативных служебных слов, аббревиатур и сокращений.

Различающиеся признаки не должны исключать тождество, а быть следствием естественной вариационности, обусловленной стилистическими особенностями речевого поведения коммуниканта (пользователя социальной сети) в ситуациях коммуникации при реализации различных коммуникативных задач и репрезентации разных референтных ситуаций<sup>10</sup>. Если различие

---

<sup>9</sup> Громова А. В. Переписка в мессенджере: идентификация автора по тексту в условиях трансформации индивидуализирующих признаков // Вестник Волгоградского государственного университета. Серия 2, Языкознание. 2021. Т. 20. № 2. С. 93.

<sup>10</sup> Назарова Т. В., Громова А. В. Опыт производства автороведческих экспертиз по материалам переписок в мессенджерах // Экспертная практика. 2019. № 86. С. 14–18.

признаков выражено в форме «непредставленности» конкретных примеров проявления признака, то это может объясняться, например, отсутствием сопоставимого контекста в исследуемых текстовых сообщениях.

Важно, что для криминалистической идентификации и диагностики лиц по материалам интернет-переписка может быть проведена судебная автороведческая экспертиза. Научные основания автороведческого исследования опираются на достижения филологических дисциплин в области судебного речеведения, когнитивной лингвистики, теории речевых актов, лингвистической прагматики, коммуникативной стилистики текста, теории дискурса, лингвистической теории эмоций, семиотики, прикладной лингвистики, а также криминалистических идентификации и диагностики. «Автороведческое исследование базируется на представлении о тексте как об «интеллектуальном следе», продукте целенаправленной речевой деятельности индивида, что определяет возможность выявления совокупности признаков его автора»<sup>11</sup>.

При изучении специфики коммуникации особое место занимает речевая деятельность, использующая специальный языковой код, служащий для передачи, получения и хранения информации, воздействия на участников коммуникации, ситуацию и окружающий мир. Изменение реалий функционирования языка в сети Интернет, требует пересмотра устоявшихся методических подходов к решению типовых задач исследования речевых произведений в целях извлечения криминалистически значимой информации. Спецификой вербальной интернет-коммуникации является использование гибридной устно-письменной формы речи, которая не только сочетает в себе письменно-речевые и устно-речевые навыки, но также обладает и собственными уникальными особенностями, которые могут быть изучены комплексно на основе современного судебного речеведения<sup>12</sup>.

На современном этапе выделяются два направления в криминалистическом изучении вербальной интернет-коммуникации. Одно из них раскрывает объективные взаимосвязи речевого следа как продукта речевой деятельности с индивидуальными особенностями личности коммуниканта, выявляемые при производстве судебной автороведческой экспертизы. Второе позволяет извлекать семантические смыслы из речевого сообщения в контексте «виртуальной реальности» при проведении судебной лингвистической экспертизы. Основные теоретические положения, лежащие в основе развития названных направлений, состоят в следующем:

---

<sup>11</sup> Громова А. В. Переписка в мессенджере: идентификация автора по тексту в условиях трансформации индивидуализирующих признаков // Вестник Волгоградского государственного университета. Серия 2, Языкознание. 2021. Т. 20. № 2. С. 91.

<sup>12</sup> Галяшина Е. И. Криминалистическое исследование вербальной интернет-коммуникации: современные реалии и доказательственное значение // Научная школа уголовного процесса и криминалистики Санкт-Петербургского государственного университета: Уголовная юстиция XXI века (к 15-летию практики применения УПК РФ): Сборник статей по материалам Международной научно-практической конференции, Санкт-Петербург, 23–24 июня 2017 года / Под редакцией Н. П. Кирилловой, Н. Г. Стойко. Санкт-Петербург: Общество с ограниченной ответственностью «Центр социальных и правовых технологий», 2018. С. 309.

1) составление вербальных электронных сообщений в интернет-коммуникации формирует у пользователя сети специфические устно-письменно-речевые навыки, способствует образованию речемыслительного функционально-динамического комплекса (стереотипа) в механизме реализации дискурсивных и интеллектуальных навыков;

2) речевой след (продукт речевой деятельности) является репрезентативным носителем криминалистически значимых свойств о языковой личности, устанавливаемых на основе интегративного знания о механизме порождения речи, условиях и закономерностях речевого поведения человека и особенностях функционирования языка в ситуации интернет-коммуникации.

Таким образом, возможности извлечения криминалистически значимой информации могут быть ограничены условиями и обстоятельствами порождения текстового сообщения, а также коммуникативной интенцией автора, которая может быть сопряжена с намеренным искажением собственного речевого портрета и имитацией чужой языковой личности<sup>13</sup>. Анонимность и возможность действовать под маской другого человека высвобождают не только творческую свободу, но и развязывают злоумышленнику руки, позволяя создавать подложные записи, умышленно искажать свою речь и имитировать вербальные навыки другого человека или группы лиц. Сиюминутность мгновенного обмена сообщениями в мессенджерах облегчает коммуникацию, снимает груз ответственности за долгосрочность последствий, провоцирует девиантное поведение.

Говоря о проблемах собирания следов информационно-коммуникативной деятельности пользователей мессенджеров и социальных сетей следует обратить внимание на то, что специфика объектов речеведческих экспертиз обусловлена их символьной (знаковой) природой. Общие криминалистические рекомендации по изъятию и фиксации переписки в мессенджерах содержат требования фиксировать в протоколе индивидуальные признаки «изъятых устройств и электронных носителей информации (размер, форму, номер и т. д.), позволяющие идентифицировать их и хранящуюся на них информацию; предъявляют требования к обеспечению их сохранности, механической целостности»<sup>14</sup>. Безусловно, они в полной мере должны соблюдаться при получении объектов речеведческих исследований, однако не являются достаточными. Разработка профильных рекомендаций – наиболее актуальное направление дальнейшего развития темы, затронутой в настоящем исследовании.

---

13 Сааков Т. А. Судебная автороведческая экспертиза объектов из цифровой среды при установлении демографических характеристик автора // Законы России: опыт, анализ, практика. 2020. № 4. С. 96–104.

14 Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 120.

## Список литературы

1. Галяшина Е. И. Криминалистическое исследование вербальной интернет-коммуникации: современные реалии и доказательственное значение // Научная школа уголовного процесса и криминалистики Санкт-Петербургского государственного университета: Уголовная юстиция XXI века (к 15-летию практики применения УПК РФ): Сборник статей по материалам Международной научно-практической конференции, Санкт-Петербург, 23–24 июня 2017 года / Под редакцией Н. П. Кирилловой, Н. Г. Стойко. Санкт-Петербург: Общество с ограниченной ответственностью «Центр социальных и правовых технологий», 2018. С. 305–312.
2. Горошко Е. И., Землякова Е. А. Полиформатный мессенджер как жанр 2.0 (на примере мессенджера мгновенных сообщений Telegram) // Жанры речи. 2017. № 1 (15). С. 97–100.
3. Громова А. В. Переписка в мессенджере: идентификация автора по тексту в условиях трансформации индивидуализирующих признаков // Вестник Волгоградского государственного университета. Серия 2, Языкознание. 2021. Т. 20. № 2. С. 87–98.
4. Олиндер Н. В., Гамбарова Е. А. О результатах эксперимента «Поиск и восприятие информации о личности в сети Интернет и ее использование при расследовании преступлений» // Эксперт-криминалист. 2017. № 4. С. 29–31.
5. Кавеева А. Д., Гурин К. Е. Искусственные профили «ВКонтакте» и их влияние на социальную сеть пользователей. Журнал социологии и социальной антропологии. 2018. № 21 (2). С. 214–231.
6. Клевцов К. К. Переписка в мессенджерах как доказательство. Способы получения и оформления // Уголовный процесс. 2020. № 10. С. 42–45.
7. Литвинова Т. А., Бирюкова Е. Д., Загоровская О. В. Диагностирование пола, возраста и психологических характеристик автора письменного текста с использованием методов корпусной и компьютерной лингвистики: возможности и ограничения // Вопросы криминологии, криминалистики и судебной экспертизы. 2021. № 1 (49). С. 105–111.
8. Мухин М. Ю., Лозовская А. И. Социальная сеть как источник социолингвистических данных: лексико-статистический анализ // Вестник ЮУрГУ. Серия «Лингвистика». 2019. Т. 16. № 4. С. 38–44.
9. Назарова Т. В., Громова А. В. Опыт производства автороведческих экспертиз по материалам переписок в мессенджерах // Экспертная практика. 2019. № 86. С. 14–18.
10. Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 106–123.
11. Сааков Т. А. Алгоритм судебно-экспертного исследования демографических характеристик автора по признакам письменной речи в эпоху цифровизации // Проблемы правоохранительной деятельности. 2021. № 3. С. 14–22.

12. Сааков Т. А. Судебная автороведческая экспертиза объектов из цифровой среды при установлении демографических характеристик автора // Законы России: опыт, анализ, практика. 2020. № 4. С. 96–104.

**Elena I. Galyashina**

Doctor of Law, Doctor of Philology, professor,  
Head of Criminalistic Department  
Moscow State Law University named after O. E. Kutafin (MSAL)  
(Moscow, Russia)  
eigaljashina@msal.ru

## **CORRESPONDENCE IN MESSENGERS AS A SOURCE OF CRIMINALLY SIGNIFICANT INFORMATION: FEATURES OF COLLECTION AND RESEARCH**

**Abstract:** The article highlights the possibilities of obtaining criminally significant information based on correspondence in messengers. The author draws attention to a wide range of objects united by the collective concept of «messenger correspondence», which include not only written texts of messages, but also multimedia content, audio, video files, images, animations, etc., which determines the need to use a complex of versatile special knowledge for their collection and research.

**Keywords:** criminally significant information, correspondence, written text, audio files, video files, special knowledge.

**Ганага Виктория Сергеевна**  
Адъюнкт,  
Уральский юридический институт  
Министерства Внутренних Дел Российской Федерации  
(г. Екатеринбург, Российская Федерация)  
vikaganaga@mail.ru

## **СЛЕДСТВЕННЫЕ ДЕЙСТВИЯ, ПРОВОДИМЫЕ ПОСРЕДСТВОМ ВИДЕО-КОНФЕРЕНЦ-СВЯЗИ, КАК ИСТОЧНИК ПОЛУЧЕНИЯ ДОКАЗАТЕЛЬСТВ**

**Аннотация:** В статье анализируется предусмотренный действующим уголовно-процессуальным законодательством порядок производства некоторых следственных действий путём видео-конференц-связи. Автором указываются недостатки и пробелы действующего правового регулирования, а также предложены меры, направленные на решения возникающих в правоприменительной деятельности проблем применения норм уголовно-процессуального законодательства.

**Ключевые слова:** уголовный процесс, доказывание, очная ставка, предъявление для опознания, видео-конференц-связь, дистанционные следственные действия.

Цифровизация и достижения научно-технического прогресса активно ворвались в жизнь современного общества. Сегодня практически у каждого человека имеется аккаунт в социальных сетях, электронной почте, мессенджерах, поэтому цифровая коммуникация стала важным звеном нашей жизни.

В уголовном судопроизводстве центральной задачей органов внутренних дел, в частности органов предварительного расследования, является осуществление доказывания по уголовному делу. В рамках доказывания осуществляется сбор всей необходимой информации для всестороннего, полного и объективного расследования. При получении доказательств в уголовном процессе важное значение имеют способы коммуникации между участниками уголовного судопроизводства. На сегодняшний день можно выделить два вида коммуникации: непосредственная и опосредованная. Непосредственная коммуникация подразумевает собой общение «лицом к лицу», когда собеседники непосредственно видят друг друга, общаются без использования третьих лиц или специализированных устройств. Опосредованная коммуникация – это такой вид коммуникации, при котором стороны непосредственно не взаимодействуют друг с другом, их общение происходит при помощи посредника (третьего человека, либо при использовании технических устройств).

Одним из видов опосредованной коммуникации является компьютерно-опосредованная коммуникация. Компьютерная коммуникация между участниками уголовного судопроизводства является перспективным способом получения доказательств. Поэтому посредством компьютерно-опосредованной коммуникации могут передаваться значимые для уголовного дела сведения.

Производство следственных и процессуальных действий посредством использования информационно-телекоммуникационных технологий получило широкое распространение, начиная с пандемии COVID-19, и применяется до сих пор. Тем не менее, действующее законодательство и правоприменительная практика не смогли выработать единый механизм использования видео-конференц-связи, облегчающий работу органам внутренних дел.

Особенности проведения допроса, очной ставки, опознания путём использования систем видео-конференц-связи закреплены в ст. 189.1 УПК РФ, в которой законодатель предпринял попытку детализировать процессуальный порядок указанных следственных действий. Однако у правоприменителя возникло только больше новых вопросов.

Так, например, ч. 1 ст. 189.1 УПК РФ указывает, что следователь или дознаватель для производства некоторых следственных действий могут использовать только системы видео-конференц-связи государственных органов, осуществляющих предварительное расследование. Тем не менее, не совсем ясно, что понимать под такими системами видео-конференц-связи, потому как специально предусмотренных систем для органов предварительного расследования законом и практикой не предусмотрено. Единственным специализированным сервисом, использующимся только сотрудниками МВД России, является сервис СВКС-м на базе ИСОД МВД России. Однако, как известно, предварительное расследование осуществляется не только в подразделениях МВД России, но и иными государственными органами. В этой связи встаёт вопрос о том, какой платформой необходимо пользоваться сотрудникам, если соблюдать правила ч. 1 ст. 189.1 УПК РФ.

В соответствии с ч. 2 ст. 189.1 УПК РФ, для производства допроса, очной ставки или опознания путём использования видео-конференц-связи следователем или дознавателем, производящим предварительное расследование по конкретному уголовному делу, направляет поручение следователю, дознавателю или в орган дознания по месту нахождения лица, принимающего участие в дистанционном следственном действии, прикладывая также порядок производства данного следственного действия. Анализируя положения ч. 1 и ч. 2 ст. 189.1 УПК РФ, мы сталкиваемся с вопросом о том, какую платформу должны использовать сотрудники органов внутренних дел для производства следственных действий по видео-конференц-связи в тех случаях, когда производство предварительного расследования осуществляется одним ведомством, а поручение было направлено в иное. Несмотря на то, что в соответствии с Постановлением Правительства РФ от 08.09.2010 № 697<sup>1</sup> создана

---

<sup>1</sup> Постановление Правительства РФ от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия» // СПС «КонсультантПлюс»



единая система межведомственного электронного взаимодействия, она не содержит в себе платформы для производства межведомственной видео-конференц-связи.

В этой связи в практической деятельности сотрудники органов внутренних дел могут использовать общедоступные платформы, такие как Skype, Zoom, Discord, Google Hangouts, TrueConf, WhatsApp и другие. Указанные платформы не дают гарантии, что передаваемые в процессе дистанционного следственного или процессуального действия сведения, не будут утрачены. Кроме того, возникают вопросы относительно допустимости полученных таким образом сведений.

Сам порядок производства допроса, очной ставки или опознания при помощи видео-конференц-связи чрезмерно усложнён, требует больших временных затрат на подготовку и проведение в соответствии со всеми требованиями уголовно-процессуального законодательства. Аналогичной позиции придерживается, подчёркивая «бессистемность правовой регламентации использования видеоконференц-связи в уголовном судопроизводстве»<sup>2</sup>, М. О. Василькова. Вместе с тем, И. А. Макеева отмечает, что «возникает проблема реализации принципа законности, предусмотренного ст. 7 УПК РФ, при производстве следственных действий с использованием систем ВКС»<sup>3</sup>. Для производства дистанционных следственных действий, согласно требованиям закона, необходимо привлечение большего количества властных участников, а значит, указанные сотрудники «теряют» значительную часть своего рабочего времени, которое они могли бы использовать для раскрытия и расследования преступлений, находящихся в их производстве.

В соответствии с ч. 3 ст. 189.1 УПК РФ по месту нахождения допрашиваемого лица у участников следственного действия берётся подписка о разъяснении им прав и обязанностей, ответственности, порядка производства следственного действия, оглашении им протокола следственного действия. Действующее уголовно-процессуальное законодательство требует, чтобы указанная расписка была составлена на бумажном носителе.

Вместе с этим, закон не указывает, где и как именно должна осуществляться видеозапись: видеозапись помещения, где находится допрашиваемое лицо; видеозапись помещения, где находится сотрудник, инициирующий проведение следственного действия или запись экранов цифровых устройств. В практической деятельности осуществляется как запись экрана с цифрового устройства по месту нахождения допрашиваемого, так и

---

[Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_104665/59a1ee33e6096f0bf3fd23d27eeb41a502ed129e/](https://www.consultant.ru/document/cons_doc_LAW_104665/59a1ee33e6096f0bf3fd23d27eeb41a502ed129e/) (дата обращения: 15.05.2024).

<sup>2</sup> Василькова М. О. Некоторые вопросы использования видео-конференц-связи в уголовном процессе // Инновации. Наука. Образование. 2021. № 41. С. 416.

<sup>3</sup> Макеева И. А. Реализация принципов уголовного судопроизводства при производстве следственных действий с использованием видео-конференц-связи на досудебных стадиях процесса // Криминалистика. 2023. № 3 (44). С. 43.

видеозапись помещения, где находится допрашиваемое лицо. Подобная практика, по нашему мнению, считается корректной, потому как видео-фиксация экрана устройства и самого помещения в наибольшей степени позволяет зафиксировать отсутствие давления на допрашиваемое лицо, его состояние в момент проведения следственного действия, а также соблюдение всех законно предусмотренных требований.

Исходя из положений ст. 189.1 УПК РФ, не совсем ясно, где и кем должен быть составлен протокол следственного действия. По общему правилу, протокол составляется лицом, проводящим следственное действие, а по окончании его производства подписывается всеми участвующими лицами. В случае, если допрос, очная ставка или предъявление для опознания проводятся при использовании видео-конференц-связи, то момент подписания бумажного протокола несколько затруднён. Стоит подчеркнуть, что в ст. 189.1 УПК РФ отсутствует какое-либо указание на то, в каком виде составляется протокол и вышеуказанная расписка: бумажном или электронном.

Ввиду того, что предусмотренная действующим законодательством процедура производства допроса, очной ставки и опознания путём видео-конференц-связи несовершенна, а практика применения положений ст. 189.1 УПК РФ неоднообразна, считаем, что необходима существенная переработка положений данной нормы и их последующее закрепление в законе.

Возможное решение вышеуказанных проблем видим в следующем:

1. Реформирование портала «Госуслуги» в целях его дальнейшего использования как платформы для проведения следственных действий посредством видео-конференц-связи. Сегодня практически у каждого гражданина Российской Федерации имеется учётная запись на портале «Госуслуги», которая разработана и поддерживается государством, содержит в себе паспортные, биометрические и иные данные. Портал облегчает доступ допрашиваемого лица к сервису, на котором может проводиться следственное действие. А сотруднику, проводящему допрос, очную ставку или предъявление для опознания, целесообразно использовать свою учётную запись ИСОД МВД России, на базе которого следует создать специализированный раздел, переадресующий на платформу «Госуслуг». В таком случае будут сокращены временные затраты на производство следственного действия, отпадает необходимость привлечения дополнительных участников и направления поручения, а также решён вопрос относительно допустимости использования платформы для видео-конференц-связи.

2. Взятие расписки на согласие о производстве дистанционного следственного действия. Несомненно, далеко не каждый человек умеет пользоваться современными цифровыми устройствами, поэтому законом должно быть предоставлено право допрашиваемого лица на согласие или отказ от производства следственного действия в дистанционном режиме. Указанная расписка может быть подана как в форме электронного документа, так и в бумажном виде по поручению в орган по месту нахождения допрашиваемого.

3. Закрепление в законе порядка и правил видеозаписи. С целью удостоверения факта отсутствия или наличия давления, влияния посторонних людей на допрашиваемое лицо, видеозапись следственного действия посредством видео-конференц-связи необходима. Представляется целесообразным осуществление видеозаписи экрана следователем, а также видеозапись помещения, в котором находится допрашиваемое лицо самим допрашиваемым лицом, либо сотрудником органа по месту нахождения допрашиваемого.

4. Составление электронного протокола следственного действия. Во исполнение распоряжения МВД России № 1/9112 от 09.11.2015 «О мерах по переходу на электронный документооборот»<sup>4</sup> внедрение электронного документооборота в деятельность органов предварительного расследования является приоритетным направлением. С целью облегчения составления протокола следственного действия, проводимого путём видео-конференц-связи, считаем целесообразным его составление и подписание в электронном виде. Подписание протокола следует реализовывать посредством квалифицированной электронной подписи. Подобная практика уже реализуется при подаче электронных обращений, заявлений, представлений и ходатайств в соответствии с положениями ст. 474.1 УПК РФ.

Таким образом, существующий порядок производства допроса, очной ставки, предъявления для опознания путём видео-конференц-связи несовершенен, имеет существенные пробелы, ставящие под угрозу допустимость полученных доказательств. Нами предложена альтернативная модель производства некоторых следственных действий в дистанционном формате. Для реализации представленной модели необходима модификация портала «Госуслуги». Допрос, очная ставка, предъявление для опознания, реализуемые посредством видео-конференц-связи, могут проводиться только при наличии технической возможности и согласия допрашиваемого лица на дистанционный способ производства следственного действия. Это связано с тем, что далеко не у каждого гражданина имеется достаточный уровень навыков пользования цифровыми устройствами и сетью «Интернет», а также усиленная квалифицированная электронная подпись. Поэтому при выборе способа проведения следственного действия следователь или дознаватель, в чьём производстве находится уголовное дело, должны тщательно изучить все обстоятельства, необходимые для принятия экономически и технически обоснованного решения.

---

<sup>4</sup> О мерах по переходу на электронный документооборот: распоряжение МВД России от 9 ноября 2015 г. № 1/9112 // СПС «КонсультантПлюс» [Электронный ресурс]. URL: <https://www.consultant.ru/> (дата обращения: 15.05.2024).

## Список литературы

1. Василькова М. О. Некоторые вопросы использования видео-конференц-связи в уголовном процессе // Инновации. Наука. Образование. 2021. № 41. С. 415–418.

2. Макеева И. А. Реализация принципов уголовного судопроизводства при производстве следственных действий с использованием видео-конференц-связи на досудебных стадиях процесса // Криминалисть. 2023. № 3 (44). С. 39–44.

**Viktoriya S. Ganaga**

Adjunct,

Ural Law Institute of the Ministry of Internal Affairs of the Russian Federation  
(Yekaterinburg, Russian Federation)

vikaganaga@mail.ru

## INVESTIGATIVE ACTIONS THROUGH VIDEO CONFERENCING AS A SOURCE OF EVIDENCE

**Abstract:** The article analyzes the procedure provided for by the current criminal procedure legislation for the production of certain investigative actions by video conferencing. The author points out the shortcomings and gaps of the current legal regulation, as well as suggests measures aimed at solving problems arising in law enforcement activities in the application of norms of criminal procedure legislation.

**Keywords:** criminal trial, evidence, interrogation, confrontation, presentation for identification, video conferencing, remote investigative actions.

**Даниелян Армен Сергеевич**  
Кандидат юридических наук, генеральный директор,  
Центр правовой поддержки «Веритас»  
(г. Краснодар, Российская Федерация)  
armen1992@mail.ru

## **АДАПТАЦИЯ ЮРИДИЧЕСКОГО ОБРАЗОВАНИЯ К ЦИФРОВОЙ ЭПОХЕ: РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА**

**Аннотация:** В статье анализируются основные аспекты взаимодействия юридического образования и искусственного интеллекта (далее – ИИ), при акцентировании внимания на адаптации учебных программ к условиям цифровой эры. Обсуждаются новые вызовы для правовой системы из-за внедрения ИИ, требующие пересмотра образовательных подходов. Освещены две ключевые области модернизации: интеграция информационных технологий и подготовка специалистов для работы на стыке права и технологий. Подчеркивается необходимость развития у студентов специализированных и универсальных компетенций для адаптации к меняющейся профессиональной среде. Также затрагиваются этические аспекты использования ИИ в юридической сфере, выделяется важность управления развитием технологий на основе справедливости и транспарентности.

**Ключевые слова:** искусственный интеллект, юридическое образование, право, юридическая деятельность, юридическая профессия, цифровизация, цифровые технологии, высшее образование.

В современном мире развитие искусственного интеллекта (ИИ) оказывает значительное влияние на все сферы жизни, включая образование. Согласно данным *Global Market Insights*, объём мирового рынка ИИ в образовании в 2023 году составил около 4 миллиардов долларов США, а по прогнозам к 2032 году превысит 30 миллиардов долларов США<sup>1</sup>. Ещё более впечатляющий рост объёмов инвестиций в сферу образования за аналогичный период предсказывает *Straits Research* – 53,11 млрд. долларов США<sup>2</sup>. В связи с этим, хотелось бы обратить внимание на две разнонаправленные тенденции. Так, с одной стороны, ИИ может поддержать и обогатить процесс обучения будущих юристов, но, с другой стороны, он влечёт за собой появление новых угроз и «подводных течений» для дела подготовки специалистов в области права.

---

<sup>1</sup> AI in Education Market Report, 2032 // Global Market Insights, 2022. 64 p.

<sup>2</sup> Artificial Intelligence in Education Market // Straits research [Electronic resource]. URL: [https://straitsresearch.com/report/artificial-intelligence-in-education-market#:~:text=Market%20Overview,period%20\(2024%E2%80%932032](https://straitsresearch.com/report/artificial-intelligence-in-education-market#:~:text=Market%20Overview,period%20(2024%E2%80%932032) (дата обращения: 01.05.2024).

На сегодняшний день эксперты консолидированы во мнении, что ИИ создаёт серьёзные проблемы для права в целом и для юридической профессии в частности. Поэтому крайне важно пересмотреть существующие формы юридического образования, чтобы помочь представителям юридической профессии: 1) сформировать верное представление о проблемах, возникающих в результате широкого внедрения ИИ в мире, и 2) адаптироваться к новой, «цифровой» реальности. Существует, по крайней мере, два основных способа реализовать это на практике: во-первых, необходимо изменить существующие юридические учебные программы, и, во-вторых, предложить обязательное повышение квалификации для представителей юридической профессии<sup>3</sup>. В этой связи представляется, что учебные заведения высшей школы должны ставить перед собой задачу развивать у студентов не только фундаментальные знания, но и универсальные компетенции, которые помогут им успешно адаптироваться к выбранной профессии и самостоятельно строить свои профессиональные траектории в динамично меняющемся мире<sup>4</sup>.

Использование искусственного интеллекта потенциально предоставляет следующие возможности как для преподавателей, так и студентов:

**1. Организация и анализ учебных материалов.** Система ИИ может использоваться для обработки и структурирования больших объёмов учебной информации, что может предполагать распознавание шаблонов договоров и процессуальных документов, а также их анализ, тем самым помогая в сортировке и классификации учебных материалов.

**2. Интерактивное обучение и консультации.** Система с поддержкой ИИ может работать как виртуальный помощник, отвечая на вопросы студентов и предоставляя консультации в режиме реального времени. Она способна поддержать студентов в процессе обучения, предоставляя разъяснения, примеры и практические рекомендации. Для данных целей сегодня применимы большие языковые модели, такие как ChatGPT, Gemini, Copilot и другие.

**3. Автоматизация оценки и обратная связь.** Система ИИ может использоваться для автоматизации процесса оценивания заданий и тестов, а также для предоставления обратной связи студентам. ИИ может разрабатывать персонализированные тесты и задания, которые динамически адаптируются под ответы студентов, усложняясь или упрощаясь в зависимости от их успеваемости. Такой подход позволяет более точно оценивать уровень знаний и умений каждого студента, а также способствует более глубокому усвоению материала.

**4. Юридическая аналитика и исследования.** Системы с поддержкой ИИ могут содействовать студентам и преподавателям в проведении юридических исследований посредством предоставления доступа к базам

---

<sup>3</sup> Gordon J.-S. General Introduction // Future Law, Ethics, and Smart Technologies / ed. by J.-S. Gordon. Netherlands: Brill, 2024. P. 3.

<sup>4</sup> Воронцов С. А., Мамычев А. Ю. «Искусственный интеллект» в современной политической и правовой жизнедеятельности общества: проблемы и противоречия цифровой трансформации // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2019. Т. 11. № 4. С. 9–22.

данных судебной практики и анализа судебных решений. ИИ может использоваться для создания сетей связи между различными юридическими актами и прецедентами, выявляя неочевидные связи и зависимости. Это облегчает понимание сложных юридических вопросов и способствует более глубокому анализу законодательства и судебной практики, что особенно важно при подготовке к сложным судебным делам.

**5. Виртуальные юридические тренировки и симуляции.** Посредством использования технологий дополненной реальности AR/VR возможно создание реалистичных симуляций судебных заседаний или переговоров, что позволит студентам практиковаться в юридических процедурах в безопасной и контролируемой среде. Эти тренировки помогают студентам развивать критическое мышление, навыки аргументации и публичного выступления, что является ключевым компонентом успешной юридической практики.

Ещё более десятилетия назад Р. Сасскинд не только предсказал, что юристы возьмут на себя новые роли в юридической практике, но также утверждал, что интеграция технологий в юриспруденцию приведёт к появлению новых типов рабочих мест, таких как: 1) инженер по правовым знаниям; 2) юридический технолог; 3) аналитик юридических процессов; 4) менеджер юридических проектов; 5) специалист по юридическим данным; 6) исследования и разработки; 7) практикующий специалист по онлайн-разрешению споров; 8) консультант по юридическому управлению; 9) менеджер по юридическим рискам и др.<sup>5</sup> И время продемонстрировало, что футурологические оценки британского учёного были весьма точны, подтверждением чему может служить динамичный рост тематических магистерских программ и программ повышения квалификации на базе ведущих образовательных учреждений страны – как государственных (НИУ ВШЭ, КФУ, МГИМО, МГУ, МГЮА, СПбГУ, СГЮА), так и частных (Moscow Digital School)<sup>6</sup>.

Исследователи предлагают разнообразные формы применения ИИ в образовании: от роботизированных существ, имитирующих человеческое общение, до специализированных систем, которые предоставляют методические

---

<sup>5</sup> Susskind R. *Tomorrow's Lawyers: An Introduction to Your Future*. Oxford, 2013. 288 p.

<sup>6</sup> См.: Интеллектуальные права и право новых технологий. URL: <https://msal.ru/programs/vysshee-obrazovanie/magistratura/magisterskaya-programma-intellektualnye-prava-i-pravo-novykh-tekhnologiy> (дата обращения: 30.04.2024); Интеллектуальные права, искусственный интеллект и цифровые технологии. URL: <https://www.law.msu.ru/courses/72> (дата обращения: 30.04.2024); Магистерская программа «Цифровое право». URL: <https://www.hse.ru/ma/dlaw/> (дата обращения: 30.04.2024); Информационное право и защита данных. URL: <https://spbu.ru/postupayushchim/programms/magistratura/informacionnoe-pravo-i-zaschita-dannykh> (дата обращения: 30.04.2024); Магистр IT Law. URL: <http://www.xn--80af5bzc.xn--p1ai/ru/component/k2/item/15106-magistr-it-law>; Магистерская программа «Юрист в сфере цифровой экономики». URL: <https://kpfu.ru/law/magistratura/abiturientam/magisterskie-programmy/magisterskaya-programma-39jurist-v-sfere-cifrovoj> (дата обращения: 30.04.2024); Программа магистратуры «Правовое регулирование цифрового развития». URL: <https://pk.odin.mgimo.ru/master/pscr.html> (дата обращения: 30.04.2024); Юрист в сфере IT. URL: <https://mosdigitals.ru/courses/software-lawyer> (дата обращения: 30.04.2024).

рекомендации. Также обсуждаются гибридные и виртуальные образовательные среды, которые могут радикально изменить взаимодействие между учащимися и педагогами. В целом, интеграция ИИ в педагогику начинает «становиться полноправным направлением совершенствования этой сферы человеческой деятельности»<sup>7</sup> и рассматривается как ключ к инновационному развитию и усовершенствованию образовательного процесса.

Однако, как и любое технологическое явление, применение систем искусственного интеллекта сопряжено с определёнными рисками.

1. Как показывают опубликованные исследования, человек склонен доверять компьютеру и принимаемым им решениям больше, чем другим людям<sup>8</sup>. Люди также реже оспаривают решения, если знают, что их приняла автоматизированная система. Это является большой проблемой в контексте того факта, что многие системы на основе ИИ усиливают *предвзятость*, присутствующую в обучающих данных, и совершают сложно выявляемые ошибки.

2. Внедрение и использование ИИ в юридическом образовании несёт с собой ряд *вопросов этического и правового характера*. Например, аспекты конфиденциальности и защиты данных становятся особенно актуальными, когда речь идёт о сборе и обработке персональных данных студентов, в особенности несовершеннолетних. При этом важно отметить, что ИИ должен рассматриваться как вспомогательный инструмент, а не замена преподавателей – человеческое оценивание и экспертиза остаются необходимыми для обеспечения качества образования и развития навыков, таких как критическое мышление и этическое рассуждение.

3. *Ещё одним вызовом являются галлюцинации ИИ*<sup>9</sup>. В рамках юридического образования это может найти отражение в неправильной

---

<sup>7</sup> Коляда М. Г., Бугаева Т. И. Искусственный интеллект как движущая сила совершенствования и инновационного развития в образовании и педагогике // Информатика и образование. 2019. № 10. С. 21–30.

<sup>8</sup> Bogert E., Schechter A. & Watson R.T. Humans rely more on algorithms than social influence as a task becomes more difficult // Science reports. 2021. Vol. 11. Pp. 1–9. DOI: 10.1038/s41598-021-87480-9.

<sup>9</sup> Объективности ради стоит отметить, что существует плюрализм в трактовке данного термина. Первоначально термин «галлюцинация в ИИ» появился в области компьютерного зрения и имел положительные коннотации, т. к. описывал методы, которые улучшали качество изображений через восстановление или добавление отсутствующих пикселей. Однако со временем термин стал использоваться для описания ошибок в моделях ИИ, в частности, при генерации текста, где результаты могут быть полностью несвязанными с исходным запросом. Группой американских исследователей (Maleki N., Padmanabhan B., Dutta K. AI Hallucinations: A Misnomer Worth Clarifying // arXiv [Electronic resource]. January 9, 2024. URL: <https://arxiv.org/abs/2401.06796v1> (дата обращения: 01.05.2024)) был проведён систематический обзор, построенный на изучении использования термина «галлюцинации» в 14 базах данных. Основная цель была выяснить, как термин применяется в различных областях ИИ и насколько его использование является последовательным и адекватным. Результаты исследования показали, что определения «галлюцинаций в ИИ» значительно различаются, т. к. в одних случаях термин применяется для описания полезных аспектов ИИ,



интерпретации данных и ошибок в алгоритмах, что может привести к порокам в рекомендациях и выводах. Негативные последствия включают некорректную интерпретацию правовых норм, предвзятые решения, отсутствие прозрачности и ответственности, нарушение конфиденциальности и конфликт интересов. Думается, что изложенное чётко подпадает под то, что В. В. Лазарев охарактеризовал как «цифровое слабоумие»<sup>10</sup>. Дополнительно, мы сталкиваемся с т. н. *проблемой «чёрного ящика»*, логически вытекающей из галлюционирования. Сущность проблемы заключается в том, что часто непонятно, как ИИ приходит к определённым выводам или результатам. В образовательной сфере такая неопределённость может быть критичной, поскольку ошибки в обучении порождают риск серьёзных последствий. В отличие от опытных специалистов, которые могут анализировать и корректировать выводы ИИ, студенты не всегда способны распознать ошибки и отсеять неверную информацию, что подрывает всю ценность образовательного процесса, превращая его в профанацию. Поэтому важно использовать ИИ в образовании осторожно, принимая его выводы как исходный материал или рекомендации, которые требуют дальнейшего анализа и проверки<sup>11</sup>.

Исследования показывают, что от 22 до 23 % задач, выполняемых юристами, могут быть автоматизированы<sup>12</sup>, а до 39 % рабочих мест в юридической сфере могут исчезнуть из-за автоматизации<sup>13</sup>. Это заставляет задуматься о будущем юридической практики и образования, которые зависят от способности профессии адаптироваться к юридическим технологиям. В исследовании, проведённом компанией *LawGeex*, инструмент ИИ сравнивался с юристами в задаче проверки контрактов. ИИ показал лучшие результаты, идентифицируя проблемы в 94 % случаев, в то время как юристы – в 85 %. Кроме того, ИИ выполнял задачу за 26 секунд, в то время как юристам требовалось в среднем 92 минуты. В реальных условиях, где юристы выполняют множество задач одновременно, этот временной разрыв может быть ещё больше<sup>14</sup>.

---

а в других – для указания на серьёзные ошибки или недостатки. В данном контексте особую важность приобретает унификация понятийно-категориального аппарата в сфере ИИ и преодоления существующей путаницы для улучшения понимания и эффективности проводимых исследований и практического применения ИИ в различных областях.

<sup>10</sup> Лазарев В. В. Юридическая наука в свете перспектив цифровизации // Журнал российского права. 2023. № 2. С. 5–19.

<sup>11</sup> Кочкин М. Создание образовательных симуляторов с GPT // ChatGPT для юриста и преподавателя: расшифровка материалов открытого семинара из цикла «Как учить юристов» (факультет права НИУ ВШЭ, 3 апреля 2023 года). М.: Центр трансформации юридического образования факультета права НИУ ВШЭ, 2023. С. 24–25.

<sup>12</sup> Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation: executive summary. McKinsey Global Institute, 2017. 28 p.

<sup>13</sup> Hill J. Deloitte Insight: Over 100,000 Legal Roles to be Automated // Legal Insider [Electronic resource]. March 16, 2016. URL: <https://legaltechnology.com/2016/03/16/deloitte-insight-over-100000-legal-roles-to-be-automated> (дата обращения: 01.05.2024).

<sup>14</sup> Leary K. The Verdict Is In: AI Outperforms Human Lawyers in Reviewing Legal Documents // Futurism [Electronic resource]. February 27, 2018. URL: <https://futurism.com/ai-contracts-lawyers-lawgeex> (дата обращения: 01.05.2024).

Отчасти можно разделить беспокойство представителей преподавательского корпуса по поводу того, что в ближайшей перспективе вопросы разработки, проверки и оценки экзаменационных работ отойдут ИИ – объективному и бесстрастному. «Это будет совершенно иная реальность и иная роль преподавателя, если он ещё останется в учебном процессе»<sup>15</sup>. Однако в предыдущих исследованиях мы уже отмечали, что не поддерживаем алармизма некоторых учёных, считающих, что ИИ *ad portas* – это предвестник гибели юридической профессии в целом<sup>16</sup>. Вопросы права и юридической квалификации не могут быть полностью переданы ИИ без оценки со стороны юриста-человека, будь то судья, адвокат или преподаватель юридических дисциплин.

Процесс интеграции цифровых технологий в юридическое образование, по мнению Е. А. Алферовой, предполагает решение двух задач: во-первых, освоение цифровых компетенций и навыков, которые преподаватели высших учебных заведений передают обучающимся и требуют от них; во-вторых, более глубокой рефлексии о будущем юридической профессии в различных контекстах и профессиональных реалиях<sup>17</sup>.

В соответствии с Пекинским консенсусом по искусственному интеллекту и образованию, принятым под эгидой ЮНЕСКО:

- развитие ИИ должно осуществляться под контролем человека и быть ориентировано на людей;
- развёртывание ИИ должно отвечать интересам людей и способствовать укреплению их потенциала;
- разработка ИИ должна руководствоваться принципами этики, справедливости, транспарентности, подотчётности и отказа от дискриминации;
- воздействие ИИ на людей и общество должно контролироваться и оцениваться на всех этапах производственно-сбытовой цепочки<sup>18</sup>.

Учёные-правоведы отмечают, что в настоящее время первоочерёдным является поиск ответов на ряд вопросов: как выстроить систему дисциплин и учебных программ по юриспруденции ИИ? Как составить учебники и материалы по ИИ-правоведению? В долгосрочной перспективе преподавательскому корпусу придётся столкнуться с проблемами ИИ в своих предметных областях,

---

<sup>15</sup> Лонская С. В. Практическая методика обучения в условиях цифровой трансформации: история права в высшей школе: учебно-методическое пособие. М., 2024. С. 173.

<sup>16</sup> Даниелян А. С. Искусственный интеллект и право будущего: риски и возможности // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2024. Т. 10 (76). № 1. С. 39–45; Даниелян А. С. К вопросу о преимуществах и рисках применения искусственного интеллекта в юриспруденции // Образование и право. 2024. № 2. С. 472–476.

<sup>17</sup> Алферова Е. В. Дилеммы юридического образования в контексте цифровизации // Право и управление. XXI век. 2022. № 18 (2). С. 14–21.

<sup>18</sup> Пекинский консенсус по искусственному интеллекту и образованию: итоговый документ Международной конференции (2022) // Пекинский консенсус по искусственному интеллекту и образованию. Пекин: Международная конференция по искусственному интеллекту и образованию. URL: <https://www.unesco.org/ru/digital-education/artificial-intelligence> (дата обращения: 01.05.2024)

отдельных курсах (возможно, курсы теории права и истории смогут выжить)<sup>19</sup>. Поэтому в данном случае большинству преподавателей-юристов, возможно, придётся заняться обновлением своего резерва знаний и усилением междисциплинарных исследований.

Нам же видятся весьма практичными и перспективными три идеи по совершенствованию юридического образования в срезе применения ИИ, предложенные У. Коннеллом и М. Хэмлин<sup>20</sup>:

*Во-первых, определить навыки, которые необходимы и будут необходимы для успешной юридической практики в XXI веке.* Здесь стоит выделить три направления, по которым юридические школы должны обучать студентов: 1) критический анализ; 2) творческое решение сложных проблем и 3) эмоциональная клиентоориентированность. Зарубежными исследователями отмечается в данной связи, что креативность и эмпатия – те области, в которых ИИ не может превзойти человека<sup>21</sup>. Схожая мысль высказывается и в российской правовой доктрине: «Творческий труд и совесть юриста незаменимы»<sup>22</sup>.

*Во-вторых, интегрировать курсы или программы, обучающие использованию ИИ в правовое поле.* Юридические школы должны предоставить формальное обучение по использованию ИИ, разработав специальные курсы и обеспечив доступ к соответствующим программам. Для сохранения конкурентоспособности, юридическим школам необходимо сосредоточиться на обучении студентов современным навыкам, а не только на прошлых успешных подходах. Обеспечение сильной учебной программы по ИИ поможет привлечь студентов и сохранить конкурентоспособность школы на рынке образования.

*В-третьих, поощрять большее партнёрство между студентами-юристами и технологическими стартапами.* Юридические школы могут решить эту проблему, предлагая студентам возможность работать с юридическими компаниями и помогать стартапам и новым технологическим компаниям. Юридическим школам также следует пересмотреть учебные программы и внедрить обучение использованию ИИ в юридической профессии. Это поможет привлечь будущих студентов-юристов, которые хотят быть подготовленными к новому юридическому миру, где ИИ становится неотъемлемой частью работы. Примером такого сотрудничества является недавно подписанное соглашение между НИУ ВШЭ и Сбербанком о сетевой

---

<sup>19</sup> Hu T., Lu H. Study on the Influence of Artificial Intelligence on Legal Profession // 5th International Conference on Economics, Management, Law and Education (EMLE 2019). 2019. Pp. 964–968.

<sup>20</sup> Connell W., Hamlin M. Black Artificial Intelligence and Legal Education // The Computer & Internet Lawyer. 2019. Vol. 36. № 5. Pp. 15–17.

<sup>21</sup> Sundquist C. B. Artificial Intelligence, Algorithmic Knowledge and the Future of Law Schools // A Place to Discuss Best Practices for Legal Education [Electronic resource]. April 9, 2018. URL: <https://bestpracticeslegaled.com/2018/04/09/artificial-intelligence-algorithmic-knowledge-and-the-future-of-law-schools> (дата обращения: 01.05.2024)

<sup>22</sup> Еременко Р. С. Искусственный интеллект и юрист: дуэль или коворкинг? // Актуальные проблемы гражданского права. 2019. № 1-2 (13-14). С. 238.

форме реализации образовательной программы бакалавриата «Юриспруденция: цифровой юрист»<sup>23</sup>.

Ещё одна проблема связана с общемировой тенденцией – у нынешних студентов, как правило, выявляются характеристики, не соответствующие творческому типу обучения<sup>24</sup>. Проведённые исследования демонстрируют, что на рубеже 2000-х гг., произошла заметная качественная трансформация в типе интеллекта подростков. Ранее преобладавшая логическая систематизация информации на основе понятийного мышления была замещена формально-образными обобщениями, при которых суть явлений не выделяется и не понимается, хотя большие объёмы информации могут удерживаться в памяти<sup>25</sup>.

Для «нового» типа интеллекта характерны<sup>26</sup>:

- поверхностность мышления;
- пренебрежение качественным анализом;
- абсолютизация методов математического анализа;
- ошибки при принятии решений из-за непонимания причинно-следственных связей;
- неадекватность перспективного планирования и прогностической деятельности в целом.

Можно констатировать, что происходит замена аналитического юридического мышления на механическое<sup>27</sup>. Очевидно, что новые времена (технологии) требуют новых решений (образовательных методик). Новый подход представляет собой интеграцию проблемных, сократовских и дискуссионных методов.

Исследования подтверждают: некоторые общие навыки, которые ранее приобретались в юридических школах, могут быть заменены автономными системами. Особенно рутинные и повторяющиеся задачи, такие как анализ законодательных материалов, подготовка документов и простой анализ судебных решений, могут быть эффективно выполнены компьютерными системами. В свете этих изменений, юридическим школам следует уделить больше внимания развитию сложных навыков, которые не могут быть легко

---

<sup>23</sup> Факультет права НИУ ВШЭ и ПАО «Сбербанк» подписали договор о сотрудничестве // Высшая школа экономики. [Электронный ресурс]. 15 февраля 2024. URL: <https://pravo.hse.ru/news/896870403.html> (дата обращения: 29.04.2024).

<sup>24</sup> Louw A. Artificial Intelligence (AI) in non-law student training // Law and Industry 4.0 – Selected Perspectives on a New Scholarship of Teaching and Learning / eds. by M. Njotine, L. G. Mpedi. Johannesburg, 2020. Pp. 59–70.

<sup>25</sup> Ясюкова Л. А. Изменение структуры интеллекта подростков с 1990 по 2020 годы // Психологическая газета [Электронный ресурс]. 16 сентября 2020. URL: <https://psy.su/feed/8560/> (дата обращения: 29.04.2024).

<sup>26</sup> Ясюкова Л. А. Изменение структуры интеллекта подростков с 1990 по 2020 годы // Психологическая газета [Электронный ресурс]. 16 сентября 2020. URL: <https://psy.su/feed/8560/> (дата обращения: 29.04.2024).

<sup>27</sup> Умнова-Конюхова И. А., Алешкова И. А. Современное юридическое образование: актуальные вопросы внедрения цифровых технологий // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право: Реферативный журнал. 2022. № 2. С. 25–39.

автоматизированы (например, медиация, переговоры, судебное представительство и другие сферы, требующие эмоционального интеллекта, этики и эмпатии)<sup>28</sup>.

Говоря об адаптации юридического образования к вызовам ИИ следует выделить два основных вектора в данном вопросе:

- пересмотр образовательных программ по юридическим направлениям;
- обязательное повышение квалификации судей, юристов-практиков.

1) Разработка первого компонента, направленного на **изменения существующих юридических учебных программ**, предполагает:

а) *введения обязательных курсов по цифровым технологиям и искусственному интеллекту*. Успешное достижение данной задачи требует выполнения ряда условий: во-первых, требуется внести изменения в изучение права с целью его *междисциплинарности*. Как отмечают А. В. Малько и А. Ю. Саломатин, усиления междисциплинарных связей и организация гибридных образовательных профилей является потребностью в подготовке юристов, т. к. на перманентно трансформирующемся рынке труда востребованы специалисты с глубокими знаниями в сложных областях. Такие знания не только повышают качество профессиональных навыков из-за их многоаспектности, но и предоставляют дополнительные гарантии занятости<sup>29</sup>. Это предполагает включение информатики, робототехники и этики в учебную программу по юриспруденции. Интенциональность указанного действия заключается в предоставлении студентам достаточных знаний для понимания и оценки основных проблем, связанных с применением ИИ. Во-вторых, студенты-юристы должны иметь достаточное *понимание технологических контекстов*, связанных с ИИ и правом. Они должны посещать вводные курсы по информатике и этике, чтобы получить необходимые знания и компетенции, чтобы повысить свою квалификацию как юристов. В-третьих, обязательные курсы по цифровым технологиям должны помочь студентам-юристам понять проблемы и особенности ИИ в целом и их влияние на юридическую профессию. *Уяснение природы ИИ* позволит адекватно осознавать основные проблемы, связанные с широким использованием ИИ в обществе, и сможет обеспечить основу для справедливого и объективного осуществления правоприменительной деятельности его субъектами<sup>30</sup>.

б) *повышения уровня осведомленности об этических проблемах применения искусственного интеллекта в юридической деятельности*. Утилитарно целью является предоставление возможности студентам-юристам

---

<sup>28</sup> Abdul Ghani A. I. M. Challenges for legal education in the era of I.R. 4.0. // UUM Journal of Legal Studies. 2020. Vol. 11 (2). P. 27–51.

<sup>29</sup> Малько А. В., Саломатин А. Ю. Юридическое образование в глобализирующемся обществе // Известия высших учебных заведений. Известия высших учебных заведений. Правоведение. 2017. № 5. С. 26.

<sup>30</sup> Fornasier M. O. Legal education in the 21st century and the artificial intelligence // Revista Opinião Jurídica. 2021. Vol. 19. № 31. Pp. 1–32; Surden H. What to Teach Law Students About Artificial Intelligence and Law? // Northwestern Law Review Online (Bridges II). 2017. URL: <https://ssrn.com/abstract=3120123> (дата обращения: 01.05.2024).

решать базовые этические проблемы, связанные с ИИ и юриспруденцией. Это требует значительной подготовки, чтобы студенты могли компетентно принимать юридические решения, касающиеся вопросов, таких как предвзятость машин и расовое профилирование. Простое посещение вводного курса по этике недостаточно, необходимо обеспечить глубокую подготовку, чтобы студенты могли эффективно решать эти проблемы.

**2) Рассматривая вопрос об обязательном повышении квалификации судей, юристов-практиков** как ещё одном основополагающем векторе адаптации юридического образования к вызовам ИИ, стоит отметить, что на сегодня в профессиональной среде всё больше в качестве догмы утверждается позиция, что юрист будущего – междисциплинарный специалист, чья компетентность и навыки выходят далеко за рамки юридической профессии<sup>31</sup>. Для юристов, которые уже работают в своей профессии, но не имеют дополнительной подготовки в области ИИ и права, крайне важно посещать обязательные курсы повышения квалификации. Для избежания несправедливых судебных решений, важно разработать междисциплинарные и онлайн-курсы, которые помогут судьям и судебным представителям глубже понять сложности, связанные с ИИ в праве. Неадекватное понимание проблемных аспектов может привести к ошибкам в судопроизводстве и подорвать авторитет судебной власти.

Следует также подчеркнуть, что рассмотренные в работе тенденции и предложения не являются специфичными для России. Например, австралийский правовед Дж. Уэбб выделил пять ключевых принципов для интеграции информационных технологий в юридическое образование<sup>32</sup>:

1) введение темы «Право и технологии» в учебные программы юридических дисциплин для уяснения студентами когерентности цифровых технологий и права;

2) междисциплинарное сотрудничество юристов и специалистов из других областей;

3) применение дизайнерского мышления к решению юридических проблем;

4) изучение этических вопросов, связанных с информационными технологиями и правом;

5) развитие у студентов-юристов навыков критического мышления, творческого решения проблем и эффективного взаимодействия.

На сегодня можно констатировать, что вопросы применения ИИ в образовании и конкретно в юридическом образовании являются делом лишь ограниченного круга ведущих юридических школ страны, – расположенных в Москве, Санкт-Петербурге, Казане, Екатеринбурге, Саратове, – обладающих релевантным материально-техническим, организационно-правовым, научно-творческим и кадровым потенциалом. В большинстве вузов использование ИИ

---

<sup>31</sup> Gordon J.-S. General Introduction // *Future Law, Ethics, and Smart Technologies* / ed. by J.-S. Gordon. Netherlands: Brill, 2024. P. 11.

<sup>32</sup> Webb J. Information Technology and the Future of Legal Education: A Provocation // *The Griffith Journal of Law & Human Dignity*. 2019. Vol. 9. Pp. 72–104.

не получило целенаправленного характера, должной нормативной оценки и регламентации (например, в локальных актах, регулирующих порядок подготовки и защиты выпускных квалификационных работ).

Думается, что первоочередной задачей в интегрировании ИИ в сферу юридического образования является подготовка / переподготовка преподавателей юридических факультетов, на основе принципа «хочешь изменить мир – начни с себя». Кадровый ресурс – основа для гармоничного внедрения искусственного интеллекта в действующую образовательную траекторию, экономии финансовых средств учебных заведений, обеспечения этических принципов применения ИИ. В качестве же центров для подготовки кадров могут выступать учреждения, уже имеющие образовательные, методические и научные разработки и достижения по рассматриваемому вопросу (НИУ ВШЭ, СПбГУ, МГУ, МГЮА, СГЮА, УрГЮУ, КФУ).

### Список литературы

1. Алферова Е. В. Дилеммы юридического образования в контексте цифровизации // Право и управление. XXI век. 2022. № 18 (2). С. 14–21.
2. Воронцов С. А., Мамычев А. Ю. «Искусственный интеллект» в современной политической и правовой жизнедеятельности общества: проблемы и противоречия цифровой трансформации // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2019. Т. 11. № 4. С. 9–22.
3. Даниелян А. С. К вопросу о преимуществах и рисках применения искусственного интеллекта в юриспруденции // Образование и право. 2024. № 2. С. 472–476.
4. Даниелян А. С. Искусственный интеллект и право будущего: риски и возможности // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2024. Т. 10 (76). № 1. С. 39–45.
5. Еременко Р. С. Искусственный интеллект и юрист: дуэль или коворкинг? // Актуальные проблемы гражданского права. 2019. № 1-2 (13-14). С. 204–243.
6. Коляда М. Г., Бугаева Т. И. Искусственный интеллект как движущая сила совершенствования и инновационного развития в образовании и педагогике // Информатика и образование. 2019. № 10. С. 21–30.
7. Кочкин М. Создание образовательных симуляторов с GPT // ChatGPT для юриста и преподавателя: расшифровка материалов открытого семинара из цикла «Как учить юристов» (факультет права НИУ ВШЭ, 3 апреля 2023 года). М.: Центр трансформации юридического образования факультета права НИУ ВШЭ, 2023. С. 24–29.
8. Лазарев В. В. Юридическая наука в свете перспектив цифровизации // Журнал российского права. 2023. № 2. С. 5–19.

9. Лонская С. В. Практическая методика обучения в условиях цифровой трансформации: история права в высшей школе: учебно-методическое пособие. М., 2024. 219 с.
10. Малько А. В., Саломатин А. Ю. Юридическое образование в глобализирующемся обществе // Известия высших учебных заведений. Правоведение. 2017. № 5. С. 16–31.
11. Умнова-Конюхова И. А., Алешкова И. А. Современное юридическое образование: актуальные вопросы внедрения цифровых технологий // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право: Реферативный журнал. 2022. № 2. С. 25–39.
12. Abdul Ghani A. I. M. Challenges for legal education in the era of I.R. 4.0. // UUM Journal of Legal Studies. 2020. Vol. 11 (2). P. 27–51.
13. AI in Education Market Report, 2032 // Global Market Insights, 2022. 64 p.
14. Artificial Intelligence in Education Market // Straits research [Electronic resource]. URL: [https://straitsresearch.com/report/artificial-intelligence-in-education-market#:~:text=Market%20Overview,period%20\(2024%E2%80%932032](https://straitsresearch.com/report/artificial-intelligence-in-education-market#:~:text=Market%20Overview,period%20(2024%E2%80%932032) (дата обращения: 01.05.2024).
15. Bogert E., Schechter A., Watson R. T. Humans rely more on algorithms than social influence as a task becomes more difficult // Science reports. 2021. Vol. 11. Pp. 1–9. DOI: 10.1038/s41598-021-87480-9.
16. Connell W., Hamlin M. Black Artificial Intelligence and Legal Education // The Computer & Internet Lawyer. 2019. Vol. 36. № 5. Pp. 15–17.
17. Fornasier M. O. Legal education in the 21st century and the artificial intelligence // Revista Opinião Jurídica. 2021. Vol. 19. № 31. Pp. 1–32.
18. Gordon J.-S. General Introduction // Future Law, Ethics, and Smart Technologies / ed. by J.-S Gordon. Netherlands: Brill, 2024. Pp. 1–11.
19. Hu T., Lu H. Study on the Influence of Artificial Intelligence on Legal Profession // 5th International Conference on Economics, Management, Law and Education (EMLE 2019). 2019. Pp. 964–968. DOI: 10.2991/aebmr.k.191225.184.
20. Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation: executive summary. McKinsey Global Institute, 2017. 28 p.
21. Leary K. The Verdict Is In: AI Outperforms Human Lawyers in Reviewing Legal Documents // Futurism [Electronic resource]. February 27, 2018. URL: <https://futurism.com/ai-contracts-lawyers-lawgeex> (дата обращения: 01.05.2024).
22. Louw A. Artificial Intelligence (AI) in non-law student training // Law and Industry 4.0 – Selected Perspectives on a New Scholarship of Teaching and Learning / eds. by M. Njotine, L. G. Mpedi. Johannesburg, 2020. Pp. 59–70.
23. Maleki N., Padmanabhan B., Dutta K. AI Hallucinations: A Misnomer Worth Clarifying // arXiv [Electronic resource]. January 9, 2024. URL: <https://arxiv.org/abs/2401.06796v1> (дата обращения: 01.05.2024).
24. Sundquist C. B. Artificial Intelligence, Algorithmic Knowledge and the Future of Law Schools // A Place to Discuss Best Practices for Legal Education [Electronic resource]. April 9, 2018. URL:



<https://bestpracticeslegaled.com/2018/04/09/artificial-intelligence-algorithmic-knowledge-and-the-future-of-law-schools/> (дата обращения: 01.05.2024).

25. Surden H. What to Teach Law Students About Artificial Intelligence and Law? // Northwestern Law Review Online (Bridges II). 2017. URL: <https://ssrn.com/abstract=3120123> (дата обращения: 01.05.2024).

26. Susskind R. Tomorrow's Lawyers: An Introduction to Your Future. Oxford, 2013. 288 p.

27. Webb J. Information Technology and the Future of Legal Education: A Provocation // The Griffith Journal of Law & Human Dignity. 2019. Vol. 9. Pp. 72–104.

**Armen S. Danielyan**

PhD (Law), General Director,  
Legal Support Center «Veritas»  
(Krasnodar, Russian Federation)  
[armen1992@mail.ru](mailto:armen1992@mail.ru)

## **ADAPTATION OF LEGAL EDUCATION TO THE DIGITAL AGE: THE ROLE OF ARTIFICIAL INTELLIGENCE**

**Abstract:** The article analyzes the main aspects of the interaction between legal education and artificial intelligence (hereinafter referred to as AI), focusing on the progress of academic programs in the digital era. New challenges for shutdown systems due to the dangers of AI are discussed, requiring a rethinking of educational approaches. Two key areas of progress are highlighted: the integration of information technology and the training of specialists to work in the field of rights and technology. The need to develop specialized and universal competencies in students to adapt to a changing professional environment is emphasized. Ethical aspects of the use of AI in the legal field are also addressed, which examine the levels of governance of technology development based on fairness and transparency.

**Keywords:** artificial intelligence, legal education, law, legal activity, legal profession, digitalization, digital technologies, higher education.

**Денисович Вероника Владимировна**

Кандидат юридических наук, доцент, старший научный сотрудник,  
Научно-исследовательский институт цифровых технологий и права  
Казанского инновационного университета имени В. Г. Тимирязова  
(г. Казань, Российская Федерация)  
LtybctyejV1984@yandex.ru

## **ФОРМИРОВАНИЕ КОНЦЕПЦИИ МЕТАВСЕЛЕННЫХ В РОССИИ**

**Аннотация:** В статье рассмотрены основные научные подходы к представлению метавселенных. Выделяются положительные последствия внедрения указанной технологии в жизнь общества и предлагаются основные пути нормативного регулирования рассматриваемой области. Также автор не оставляет без внимания и потенциальные риски, связанные с чрезмерным, неправильным или злонамеренным использованием метавселенных.

**Ключевые слова:** метавселенные, виртуальная среда, виртуальные миры, аватар человека, цифровые технологии, цифровой человек, метаданные.

Первоначально концепция метавселенных носила футуристический характер. Многие авторы старались описать новую виртуальную реальность как нечто фантастическое, не существующее, но так необходимое человеку в будущем.

Однако уже сегодня этические и правовые аспекты, такие как конфиденциальность, отсутствие дискриминации и развивающиеся правовые рамки, определены как критические факторы, формирующие современные метавселенные (Metaverse)<sup>1</sup>, которые позволяют обеспечить цифровую доступность в мире.

Вместе с тем, на настоящий момент в России отсутствует единая концепция метавселенных. Во многом такая ситуация обусловлена стремлением человека первоначально понять, в какой сфере необходимо дать определение новому явлению. Публикациями НТЦ «Главный радиочастотный центр» при Роскомнадзоре подтверждается важность исследований в области метапространств. Организация выделила риски метавселенных, связав их со стремлением пользователей перенести в виртуальный мир свои ценности, этику и идентичность, что, по мнению разработчиков и исследователей, будет оказывать влияние на физический мир и иметь реальные негативные последствия<sup>2</sup>. Соглашаясь с таким выводом, следует отметить, что технология

---

<sup>1</sup> Othman A., Chemnad K., Hassanien A. E. [et al]. Accessible Metaverse: A Theoretical Framework for Accessibility and Inclusion in the Metaverse // Multimodal Technologies and Interaction. 2024. Vol. 8 (3). № 21. DOI: 10.3390/mti8030021.

<sup>2</sup> Reidenberg J. R. Lex Informatica: The Formulation of Information Policy Rules through Technology // Fordham Law Archive of Scholarship and History. 1997. Vol. 76. Pp. 553–593.

метавселенной, как любая иная цифровая технология, всегда нейтральна. Негативное или позитивное влияние на социум зависит только от субъекта, её создающего и использующего.

Следует привести ряд точек зрения, в которых авторы дают наиболее точные определения метавселенным. Так, с позиции К. С. Евсикова, *метавселенная – «информационная система, существующая в форме цифровой платформы и/или социальной сети, предоставляющая возможность создавать и осуществлять переход цифровых прав между пользователями, для доступа к которой физическое лицо может использовать информационные технологии виртуальной и/или дополненной реальности, а также проецировать в реальную действительность виртуальные объекты»*<sup>3</sup>. Данное определение носит комплексный характер и может применяться на нынешнем этапе становления концепции метавселенных.

Если же рассматривать энциклопедическое понимание метавселенных, то следует уточнить, что *метавселенная – интегративная экосистема виртуальных миров, предлагающих погружение в мир, где изменяется уже имеющийся опыт и создаются новые ценности с экономической, экологической, социальной и культурной точек зрения*. Она определяется как непрерывное и взаимосвязанное сочетание физической и виртуальной сфер, чему способствуют такие технологии, как виртуальная реальность и дополненная реальность, где пользователи участвуют в мультисенсорном взаимодействии в постоянных и совместно используемых иммерсивных средах<sup>4</sup>. Тем не менее, данное утверждение нуждается в уточнении.

В этой взаимосвязанной цифровой сфере пользователи могут взаимодействовать друг с другом и с созданной компьютером средой в режиме реального времени, что приводит к размыванию границ между физическим и цифровым мирами<sup>5</sup>. Часто описываемая как полностью иммерсивное и интерактивное пространство, метавселенная предлагает пользователям возможность исследовать, создавать и участвовать в различных видах деятельности<sup>6</sup>.

Следует признать тот факт, что постоянное развитие Metaverse значительно изменяет нашу повседневную жизнь, профессиональные занятия и досуг, тем самым предвещая новую эру взаимосвязанности и виртуальных исследований. Есть и другой подход в теории, согласно которому Metaverse – полностью смоделированный виртуальный мир. Однако ряд авторов полагают,

---

<sup>3</sup> Бегишев И. Р., Латыпова Э. Ю., Кирпичников Д. В. Искусственный интеллект как правовая категория: доктринальный подход к разработке дефиниции // Актуальные проблемы экономики и права. 2020. Т. 14. № 1. С. 79–91. DOI: 10.21202/1993-047X.14.2020.1.79-91.

<sup>4</sup> Mystakidis S. Metaverse // Encyclopedia. 2022. Vol. 2. Pp. 486–497.

<sup>5</sup> Huang L., Gao B., Gao M. The Metaverse Era: The Fourth Transformation in the Age of Internet Communication // Value Realization in the Phygital Reality Market: Consumption and Service under Conflation of the Physical, Digital, and Virtual Worlds / Eds. by Huang L., Gao B., Gao M.; Kobe University Monograph Series in Social Science Research. Singapore: Springer Nature, 2023. Pp. 99–123.

<sup>6</sup> Zallio M., Clarkson P. J. Designing the Metaverse: A Study on Inclusion, Diversity, Equity, Accessibility and Safety for Digital Immersive Environments // Telematics and Informatics 2022. Vol. 75. DOI: 10.1016/j.tele.2022.101909.

что метавселенные – это форма наложения дополненной реальности на реальный мир<sup>7</sup>. Предполагается, что полностью виртуальный мир будет широко использоваться для игр, общения, покупок, развлечений, бизнеса и образования. Тогда как дополненная реальность рассматривается как замена мобильным телефонам и шлюз для цифрового контента<sup>8</sup>. В настоящее время обсуждается возможность применения технологии blockchain для децентрализации и решения вопросов контроля в Metaverse<sup>9</sup>. Однако также высказываются опасения по поводу стоимости доступа, возможности дезинформации, цифрового неравенства, сохранения объектов и идентификационных данных, а также возможного негативного влияния на отношения и обязательства в реальном мире<sup>10</sup>.

Цифровизация, охватившая все сферы жизнедеятельности человека, целенаправленно создаёт новое отношение к человеку, формам его существования. В научной среде появился такой термин как «HomoDigitals» – человек цифровой<sup>11</sup>. Существование такой личности возможно в двух формах: как обычного человека с элементарными человеческими потребностями, так и в виртуальном пространстве – в метавселенной. Однако для этого необходимо наличие постоянной связи с цифровой средой<sup>12</sup>, поскольку бытие такого человека будет одновременно и неразрывно протекать в обычном и цифровом мирах с помощью технологий дополненной и виртуальной реальности. Однако есть ещё один существенный процесс – «оцифровка» профиля человека для различных целей, например анализа его эффективности, социальной активности, научного и трудового потенциала, состояния здоровья. В этой связи возникает необходимость разделить понятия или, по крайней мере, чётко выделить разницу между цифровыми технологиями в описании профиля человека и оцифрованными данными об этом же человеке<sup>13</sup>.

---

<sup>7</sup> Owusu-Antwi K., Amenuvor F. E. Understanding the Metaverse: A Review of Virtual Worlds and Augmented Reality Environments // Current Journal of Applied Science and Technology. 2023. Vol. 42 (23). Pp. 42–48. DOI: 10.9734/cjast/2023/v42i234172.

<sup>8</sup> George A. H., Fernando M., George A. S., Baskar T., Pandey D. Metaverse: The next Stage of Human Culture and the Internet // International Journal of Trendy Research in Engineering and Technology (IJARTET). 2021. Vol. 8. Pp. 1–10. DOI: 10.5281/zenodo.6548172.

<sup>9</sup> Maksymyuk T., Gazda J., Bugár G., Gazda V., Liyanage M., Dohler M. Blockchain-Empowered Service Management for the Decentralized Metaverse of Things // IEEE Access. 2022. Vol. 10. Pp. 99025–99037. DOI: 10.1109/ACCESS.2022.3205739.

<sup>10</sup> Бегисhev И. Р. Технология искусственного интеллекта: мировой опыт развития // Baikal Research Journal. 2020. Т. 11. № 3. DOI: 10.17150/2411-6262.2020.11(3).1.

<sup>11</sup> Brown J., Bailenson J., Hancock J. Misinformation in Virtual Reality // Journal of Online Trust and Safety. 2023. Vol. 1. Pp. 1–30. DOI: 10.54501/jots.v1i5.120; Pathak-Shelat M., Mehta B. The Future of Higher Education in Ethical Metaverse: Co-Existing in Virtually Enhanced Physical Reality // The Emergence of the Ethically-Engaged University / Eds. by Bosio E., Gregorutti G., International and Development Education; Cham, Switzerland: Springer International Publishing, 2023. Pp. 137–157.

<sup>12</sup> Федотов М. А. Конституционные ответы на вызовы киберпространства // Lex russica (Русский закон). 2016. № 3. С. 164–182. DOI: 10.17803/1729-5920.2016.112.3.164-182.

<sup>13</sup> Бачило И. Л. Институциональный подход к решению проблем понятийного аппарата в информационном законодательстве // Понятийный аппарат в информационном праве / отв. ред. И. Л. Бачило, Т. А. Полякова, В. Б. Наумов: кол. монография. М.: ИПП РАН: Издательство «Канон+» РООИ «Реабилитация», 2017. С. 12–28.

Тематика публикации ориентирует нас ответить на вопрос, как защитить человека в условиях нового виртуального пространства. Для ответа на вопрос необходимо первоначально определиться с тем, от чего надо защитить. Безусловно, цифровизация является благом для развития общества, а многие её процессы прочно укоренились в социальной практике<sup>14</sup>.

Обратимся к исследованиям в области психологии и медицины. Академиком И. П. Павловым было доказано, что единственным физиологическим принципом деятельности целого мозга, объясняющим целостное поведение животных и человека, является принцип условного рефлекса<sup>15</sup>. Академик П. К. Анохин доказал, что универсальным принципом всех форм живого является опережающее отражение событий действительности внешнего мира<sup>16</sup>.

Итак, человек в современном мире может расширить границы своих возможностей с использованием искусственного интеллекта и метавселенных. Основным тезисом, который следует признать является следующее: метавселенные существуют и уже используются человеком, в дальнейшем концепция метавселенных будет только расширяться и становиться научно обоснованной. Человеку необходимо обладать не только знаниями в этой области, но и комплексом норм, защищающих его и позволяющих безопасно существовать в структуре метапространства.

Права человека и сам человек должны быть защищены в условиях нового виртуального пространства. Как справедливо отмечает Д. В. Бахтеев, с созданием новых цифровых технологий и активным использованием искусственного интеллекта в жизни человека необходимо сохранить персонализацию человека, защитить его право на жизнь, здоровую окружающую среду и развитие, его рабочее место<sup>17</sup>. Все эти гарантии неминуемо повлекут изменения в трудовом, административном, семейном, гражданском, уголовном законодательстве. Так или иначе, с внедрением в широкий оборот метавселенных и участием в них человека возникнут объективные изменения всей системы права, каждой отрасли без исключения.

На этапе разработки цифровой модели общества ещё трудно предсказать все её негативные стороны, тем не менее, основываясь на существующих рисках в сфере цифровизации, можно предположить, что данная инновация изначально при плохой разработке представляет угрозу для человечества.

---

<sup>14</sup> Стратегия цифровой трансформации отрасли науки и высшего образования (утв. Минобрнауки России). // Министерство науки и высшего образования [Электронный ресурс] URL: <https://minobrnauki.gov.ru/upload/iblock/e16/dv6edzmr0og5dm57dtm0wyllrbuwtujw.pdf> (дата обращения: 20.01.2023).

<sup>15</sup> Сеченов И. М., Павлов И. П., Введенский Н. Е. Физиология нервной системы. В четырёх томах. М.: Медгиз, 1952. 580; 624; 1008; 684 с.; Ухтомский А. А. Доминанта. Статьи разных лет. 1887–1939. СПб.: Питер, 2002. 448 с.

<sup>16</sup> Анохин П. К. Биология и нейрофизиология условного рефлекса. М.: Медицина, 1968. 548 с.

<sup>17</sup> Бахтеев Д. В. Этико-правовые модели взаимоотношений общества с технологией искусственного интеллекта // Journal of Digital Technologies and Law. 2023. Т. 1. № 2. С. 520–539. DOI 10.21202/jdtl.2023.22.

К наиболее вероятным рискам, с которыми столкнётся Homo Digitalis, можно отнести утрату личного пространства, деперсонализацию и независимости. В связи с этим следует критично отнестись к тотальной цифровизации и вовремя остановить её рост.

В 2021 году Правительство Российской Федерации (РФ) на Всемирном экономическом форуме (ВЭМ) представило меморандум о создании Центра четвёртой промышленной революции в России<sup>18</sup>. Данный документ предполагает планомерное внедрение систем искусственного интеллекта в повседневную жизнь человека вплоть до имплантации чипов в головной мозг (проект Национальной технологической инициативы «Нейронет-2035»)<sup>19</sup>. Отдельное внимание метавселенным в этом проекте не уделялось, тем не менее работа в этом направлении ведётся комплексно и постоянно. Таким образом, человек обязан научиться владеть цифровыми технологиями и техникой, которые он использует в повседневной жизни.

Цифровой человек (человек в метавселенной) – это человек, не просто обладающий знаниями в области цифровых технологий, но неразрывно связанный с ними посредством цифровых аватаров, дополненной и виртуальной реальностей и других способов. Как полагает М. Грациан, для этого нужно отсканировать человеческий мозг и перенести цифровое сознание в виртуальную реальность<sup>20</sup>. Думается, что данная точка зрения в целом обоснованна.

Следует отстраниться от крайностей и признать, что человек в цифровом пространстве на современном этапе развития общества – человек, свободно владеющий цифровыми технологиями. Именно право владения цифровыми технологиями, правовой статус человека, этика поведения человека в виртуальной среде, защита от любого посягательства – вопросы, требующие правового разрешения сегодня.

Одной из существенных проблем участия человека в виртуальном пространстве является утрата собственной личности, создание коллективного разума, а также полностью контролируемого разума, т. к. все мыслительные процессы будут доступны нейросетям под управлением виртуального супермозга. Для предотвращения данной угрозы пока напрашивается одно решение – приостановить совершенствование искусственного интеллекта и отказаться от его интеграции с человеческим сознанием. Эта проблема вполне может быть решена в рамках метавселенных. Этого требует этика социальной ответственности не только профессионального участника любого правоотношения, но и любого человека. В поддержку данной инициативы выступило всё развитое мировое сообщество.

---

<sup>18</sup> Крайнов А. Л. Homo Digitalis как продукт цифровизации // Вестник Северного (Арктического) федерального университета. Серия: Гуманитарные и социальные науки. 2023. Т. 23. № 5. С. 122–129. DOI: 10.37482/2687-1505-V295.

<sup>19</sup> Бахтеев Д. В. Этико-правовые модели взаимоотношений общества с технологией искусственного интеллекта // Journal of Digital Technologies and Law. 2023. Т. 1. № 2. С. 520–539. DOI 10.21202/jdtl.2023.22.

<sup>20</sup> Бикмуллин А. Цифровая экономика как инструмент социального развития российского общества // Регион. экон. журн. 2018. № 3-4 (23-24). С. 52–54.

При разработке Metaverse приоритет должен отдаваться этическим соображениям, особенно в обеспечении доступности для людей с ограниченными возможностями, несовершеннолетних, лиц, нуждающихся в дополнительной социальной поддержке. Так, эксперты отмечают: «Очень важно, чтобы при разработке Metaverse этические соображения стояли на первом и приоритетном месте, чтобы ни один человек не был ущемлён или исключён на основании своих способностей»<sup>21</sup>.

Помимо этого, особую озабоченность вызывает вопрос конфиденциальности, особенно у людей с наличием определённых тайн, информации, которая не подлежит разглашению, полагающихся на специализированные и потенциально интрузивные вспомогательные технологии. «Конфиденциальность приобретает новое измерение в метавселенной, особенно когда мы рассматриваем пользователей, которым могут понадобиться вспомогательные технологии, глубоко интегрированные в их виртуальный опыт»<sup>22</sup>. Более того, важность конфиденциальности и безопасности данных в Metaverse обусловлена самим участием человека в данной виртуальной реальности. Здесь необходимо подчеркнуть сугубо личный характер аватаров и взаимодействий, что вызывает опасения по поводу конфиденциальности данных и возможности дискриминации на основе виртуальных представлений. Для защиты пользователей и предотвращения злоупотреблений необходимы надёжные меры безопасности и этические принципы.

Итак, метавселенная даёт возможность решить ряд существенных проблем, стоящих перед человеком, в частности, быстро удовлетворить его потребности в том виде, в котором он этого хочет. Это одна из главных движущих систем организма, остановка её работы может привести к непредсказуемым результатам. Основной задачей общества на современном этапе развития информационных и цифровых технологий в рамках защиты прав человека является дружественное отношение со всеми цифровыми технологиями, их анализ и осознание их полезности. Совершенно справедливым является тезис о том, что метавселенные – это будущая форма существования интернета. Это способ решить проблемы максимально быстро и эффективно.

### Список литературы

1. Анохин П. К. Биология и нейрофизиология условного рефлекса. М.: Медицина, 1968. 548 с.

---

<sup>21</sup> George A. H., Fernando M., George A. S., Baskar T., Pandey D. Metaverse: The next Stage of Human Culture and the Internet // International Journal of Trendy Research in Engineering and Technology (IJARTET). 2021. Vol. 8. Pp. 1–10. DOI: 10.5281/zenodo.6548172.

<sup>22</sup> Dudley J., Yin L., Garaj V., Kristensson P. O. Inclusive Immersion: A Review of Efforts to Improve Accessibility in Virtual Reality, Augmented Reality and the Metaverse // Virtual Reality. 2023. Vol. 27. Pp. 2989–3020. DOI: 10.1007/s10055-023-00850-8.

2. Бахтеев Д. В. Этико-правовые модели взаимоотношений общества с технологией искусственного интеллекта // *Journal of Digital Technologies and Law*. 2023. Т. 1. № 2. С. 520–539. DOI 10.21202/jdtl.2023.22.
3. Бачило И. Л. Институциональный подход к решению проблем понятийного аппарата в информационном законодательстве // *Понятийный аппарат в информационном праве* / отв. ред. И. Л. Бачило, Т. А. Полякова, В. Б. Наумов: кол. монография. М.: ИГП РАН: Издательство «Канон+» РООИ «Реабилитация», 2017. С. 12–28.
4. Бегишев И. Р. Технология искусственного интеллекта: мировой опыт развития // *Baikal Research Journal*. 2020. Т. 11. № 3. DOI: 10.17150/2411-6262.2020.11(3).1
5. Бегишев И. Р., Латыпова Э. Ю., Кирпичников Д. В. Искусственный интеллект как правовая категория: доктринальный подход к разработке дефиниции // *Актуальные проблемы экономики и права*. 2020. Т. 14. № 1. С. 79–91. DOI: 10.21202/1993-047X.14.2020.1.79-91
6. Бикмуллин А. Цифровая экономика как инструмент социального развития российского общества // *Регион. экон. журн*. 2018. № 3-4 (23-24). С. 52–54.
7. Крайнов А. Л. Номо Digitals как продукт цифровизации // *Вестник Северного (Арктического) федерального университета. Серия: Гуманитарные и социальные науки*. 2023. Т. 23. № 5. С. 122–129. DOI: 10.37482/2687-1505-V295.
8. Некрасов А. С., Некрасов С. И., Некрасова Н. А., Клепацкий В. В. От «человека информационного» к «человеку цифровому» // *Вестник университета Российской академии образования*. 2019. № 3. С. 4–10.
9. Сеченов И. М., Павлов И. П., Введенский Н. Е. Физиология нервной системы. В четырёх томах. М.: Медгиз, 1952. 580; 624; 1008; 684 с.
10. Ухтомский А. А. Доминанта. Статьи разных лет. 1887–1939. СПб.: Питер, 2002. 448 с.
11. Федотов М. А. Конституционные ответы на вызовы киберпространства // *Lex russica (Русский закон)*. 2016. № 3. С. 164–182. DOI: 10.17803/1729-5920.2016.112.3.164-182.
12. Brown J., Bailenson J., Hancock J. Misinformation in Virtual Reality // *Journal of Online Trust and Safety*. 2023. Vol. 1. Pp. 1–30. DOI: 10.54501/jots.v1i5.120.
13. Dudley J., Yin L., Garaj V., Kristensson P. O. Inclusive Immersion: A Review of Efforts to Improve Accessibility in Virtual Reality, Augmented Reality and the Metaverse // *Virtual Reality*. 2023. Vol. 27. Pp. 2989–3020. DOI: 10.1007/s10055-023-00850-8.
14. George A. H., Fernando M., George A. S., Baskar T., Pandey D. Metaverse: The next Stage of Human Culture and the Internet // *International Journal of Trendy Research in Engineering and Technology (IJARTET)*. 2021. Vol. 8. Pp. 1–10. DOI: 10.5281/zenodo.6548172.
15. Huang L., Gao B., Gao M. The Metaverse Era: The Fourth Transformation in the Age of Internet Communication // *Value Realization in the Phygital Reality*



Market: Consumption and Service under Conflation of the Physical, Digital, and Virtual Worlds / Eds. by Huang L., Gao B., Gao M.; Kobe University Monograph Series in Social Science Research. Singapore: Springer Nature, 2023. Pp. 99–123.

16. Maksymyuk T., Gazda J., Bugár G., Gazda V., Liyanage M., Dohler M. Blockchain-Empowered Service Management for the Decentralized Metaverse of Things // IEEE Access. 2022. Vol. 10. Pp. 99025–99037. DOI: 10.1109/ACCESS.2022.3205739.

17. Mystakidis S. Metaverse // Encyclopedia. 2022. Vol. 2. Pp. 486–497.

18. Othman A., Chemnad K., Hassanien A. E. [et al]. Accessible Metaverse: A Theoretical Framework for Accessibility and Inclusion in the Metaverse // Multimodal Technologies and Interaction. 2024. Vol. 8 (3). № 21. DOI: 10.3390/mti8030021.

19. Owusu-Antwi K., Amenuvor F. E. Understanding the Metaverse: A Review of Virtual Worlds and Augmented Reality Environments // Current Journal of Applied Science and Technology. 2023. Vol. 42 (23). Pp. 42–48. DOI: 10.9734/cjast/2023/v42i234172.

20. Pathak-Shelat M., Mehta B. The Future of Higher Education in Ethical Metaverse: Co-Existing in Virtually Enhanced Physical Reality // The Emergence of the Ethically-Engaged University / Eds. by Bosio E., Gregorutti G., International and Development Education; Cham, Switzerland: Springer International Publishing, 2023. Pp. 137–157.

21. Reidenberg J. R. Lex Informatica: The Formulation of Information Policy Rules through Technology // Fordham Law Archive of Scholarship and History. 1997. Vol. 76. Pp. 553–593.

22. Zallio M., Clarkson P. J. Designing the Metaverse: A Study on Inclusion, Diversity, Equity, Accessibility and Safety for Digital Immersive Environments // Telematics and Informatics 2022. Vol. 75. DOI: 10.1016/j.tele.2022.101909.

### **Veronika V. Denisovich**

PhD (in Law), Associate Professor, Senior Researcher,  
Research Institute of Digital Technologies and Law  
Kazan Innovation University named after V. G. Timiryasov  
(Kazan, Russian Federation)  
LtybctyejV1984@yandex.ru

## **SHAPING THE CONCEPT OF METAVERSE IN RUSSIA**

**Abstract:** The article considers the main scientific approaches to the representation of metauniverses. The positive consequences of the introduction of this technology into the life of society are emphasized and the main ways of normative regulation of this area are proposed. The author also does not ignore potential risks associated with excessive, incorrect or malicious use of meta-universes.

**Keywords:** meta universes, virtual environment, virtual worlds, human avatar, digital technologies, digital man, metadata.

**Довгань Ксения Евгеньевна**

Кандидат юридических наук, ведущий научный сотрудник,  
Алтайский государственный университет  
(г. Барнаул, Российская Федерация)  
dok2122@bk.ru

## **ПРОБЛЕМЫ ТОЛКОВАНИЯ ИНФОРМАЦИОННЫХ ПРАВООТНОШЕНИЙ С ТОЧКИ ЗРЕНИЯ ЮРИДИЧЕСКОЙ КАЗУИСТИКИ\***

**Аннотация:** Рамочное правовое регулирование информационных правоотношений создаёт правовую неопределённость для правоприменителей. Необходим единый подход нормотворчества, позволяющий обеспечить эффективность правового регулирования. Представляется, что правовое регулирование информационных правоотношений должно осуществляться на основе сочетания рамочного и казуистического нормотворчества в зависимости от особенностей конкретных общественных правоотношений.

**Ключевые слова:** рамочное правовое регулирование, юридическая казуистика, информационные технологии, правовое регулирование, национальные проекты.

При оценке юридической техники нормативных правовых актов, регламентирующих информационные правоотношения, следует подчеркнуть достаточное количество общих, абстрактных правовых норм. В отдельных актах предмет правового регулирования не конкретизирован, а определяется сферой общественных отношений. Информационные правоотношения в определённой мере регламентируются при помощи рамочного правового регулирования<sup>1</sup>, что проявляется в том числе в наличии большого числа относительно определённых норм. Такой подход к регламентации создаёт правовую неопределённость, которую можно проследить, например, в программных документах, актах стратегического характера и т. д.

Представляется, что казуистический приём изложения правовых актов позволит в определённой мере снизить описанное явление. Вместе с тем, необходимо обеспечить разумное сочетание: с одной стороны, нельзя полностью исключать рамочные нормы, которые позволяют, например, закреплять обобщённые родовые понятия, и с другой, необходимо ввести конкретные

---

\* Исследование выполнено за счёт гранта Российского научного фонда № 24-28-01400, <https://rscf.ru/project/24-28-01400/>.

<sup>1</sup> Довгань К. Е. Рамочное регулирование информационных технологий в Российской Федерации // Технологии XXI века в юриспруденции: Материалы четвертой международной научно-практической конференции, Екатеринбург, 20 мая 2022 года / Отв. редактор: Д. В. Бахтеев. Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2022. С. 59–64.

нормы, направленные на закрепление фактических обстоятельств путём указания индивидуальных признаков правоотношений. Казуистичное изложение правовых норм позволит снизить объём судебного усмотрения и, соответственно, судебных ошибок. Поскольку, как показывает проведённое нами исследование, количество дел в нагрузке у судьи влияет в том числе на качество выносимых решений.

На законодательном уровне необходимо сделать акцент на установление и уточнение пределов правового регулирования информационных правоотношений, которые определяются его инструментарием, определённым набором правовых норм и их свойствами. Например, при рамочном правовом регулировании пределы устанавливаются временными, пространственными, субъектными, компетентностными критериями. Кроме того, конституционное и процессуальное законодательство напрямую закрепляет возможности аутентичного толкования. Например, ст. 83 ФКЗ «О Конституционном Суде Российской Федерации»<sup>2</sup>, ст. 202 Гражданского процессуального кодекса Российской Федерации<sup>3</sup> и др.

Таким образом, информационные правоотношения отличаются сложным междисциплинарным характером. Представляется, что правовое регулирование информационных правоотношений должно осуществляться на сочетании рамочного и казуистического нормотворчества, объём каждого из которых необходимо определять в зависимости от особенностей конкретных общественных правоотношений.

### **Список литературы**

1. Довгань К. Е. Рамочное регулирование информационных технологий в Российской Федерации // Технологии XXI века в юриспруденции: Материалы четвёртой международной научно-практической конференции, Екатеринбург, 20 мая 2022 года / Отв. редактор: Д. В. Бахтеев. Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2022. С. 59–64.

**Ksenia E. Dovgan**  
PhD (Law), Leading Researcher,  
Altai State University  
(Barnaul, Russian Federation)  
dok2122@bk.ru

---

<sup>2</sup> Федеральный конституционный закон от 21.07.1994 № 1-ФКЗ «О Конституционном Суде Российской Федерации» // Собрание законодательства РФ. 1994. № 13. Ст. 1447.

<sup>3</sup> «Гражданский процессуальный кодекс Российской Федерации» от 14.11.2002 № 138-ФЗ // Собрание законодательства РФ. 2002. № 46. Ст. 4532.

## **PROBLEMS OF INTERPRETATION OF INFORMATION LEGAL RELATIONS FROM THE POINT OF VIEW OF LEGAL CASUISTRY**

**Abstract:** The framework legal regulation of information legal relations creates legal uncertainty for law enforcers. A unified approach to rulemaking is needed to ensure the effectiveness of legal regulation. It seems that the legal regulation of information legal relations should be carried out on a combination of framework and casuistic rule-making, depending on the characteristics of specific social legal relations.

**Key words:** framework legal regulation, legal casuistry, information technology, legal regulation, national projects.

**Жевняк Оксана Викторовна**

Кандидат юридических наук, доцент кафедры правового регулирования  
экономической деятельности,

Уральский федеральный университет  
имени первого Президента России Б. Н. Ельцина  
(г. Екатеринбург, Российская Федерация)

## **ПРАВОВОЙ РЕЖИМ ПРОГРАММНО-АППАРАТНЫХ КОМПЛЕКСОВ**

**Аннотация:** В статье исследуется понятие программно-аппаратных комплексов, их легальная дефиниция, правовой режим, который включает публично-правовые нормы, направленные на охрану информационной безопасности государства и обеспечение импортозамещения. Делается вывод о том, что программно-аппаратные комплексы представляют собой сложные объекты, включающие программы для ЭВМ и оборудование (ЭВМ, электронные устройства), при этом функционирование комплекса возможно только через сочетание этих элементов. Объективное существование таких комплексов, других подобных сложных объектов и их участие в гражданском обороте требуют отражения их в перечне объектов гражданских прав и включения в их частно-правовой режим признака неделимости.

**Ключевые слова:** программно-аппаратные комплексы, аппаратно-программные комплексы, правовой режим, правовое регулирование, сложные объекты.

С 1 января 2023 г. в правовое поле введена дефиниция программно-аппаратного комплекса, а также приняты нормы права, регулирующие отношения по поводу регистрации этих комплексов в реестре отечественного программного обеспечения, их использования на объектах критической информационной инфраструктуры, осуществления государственных закупок по поводу них. Определение было включено в Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»<sup>1</sup> (эти изменения были приняты Постановлением Правительства РФ от 28 декабря 2022 г. № 2461<sup>2</sup>).

---

<sup>1</sup> Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (с изм. и доп.) // СПС «Гарант». URL: <https://base.garant.ru/71252170/> (дата обращения: 13.05.2024).

<sup>2</sup> Постановление Правительства РФ от 28 декабря 2022 г. № 2461 «О внесении изменений в постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 и признании утратившими силу отдельных положений некоторых актов Правительства Российской Федерации» // СПС «Гарант». URL: [https://base.garant.ru/406060493/#block\\_1021](https://base.garant.ru/406060493/#block_1021) (дата обращения: 13.05.2024).

Появление данного определения пока не осмыслено в научной юридической литературе, где термин «программно-аппаратные комплексы» использовался и до этого. Кроме того, в литературе и правовых актах встречались иные подобные термины, без анализа их разграничения. Набор схожих категорий достаточно обширен, однако определённости в их использовании не существует. Например, в диссертационном исследовании Д. Е. Матыцина, посвящённом заключению дистанционных инвестиционных сделок через инвестиционные платформы и биржи, можно встретить такие термины, как: программно-аппаратные имущественные комплексы, программно-аппаратный комплекс, аппаратно-программный комплекс, комплексы программно-аппаратных средств, программно-аппаратные средства, программно-аппаратное обеспечение<sup>3</sup>. Не вносит ясности попытка разграничения понятий программно-аппаратных комплексов (ПАК) и аппаратно-программных комплексов (АПК) в работе И. Николаева<sup>4</sup>. Представляется, что использование этих двух терминов является излишним.

П. У. Кузнецов отмечает, что в индустриальный интернет входят программно-аппаратные средства<sup>5</sup>, Е. М. Андреева называет среди компонентов выпуска и оборота цифровых валют комплексы программно-аппаратных средств<sup>6</sup>. Согласно ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» «автоматизированная система управления – это комплекс программных и программно-аппаратных средств...»<sup>7</sup>. В п. 10 ст. 8 Федерального закона от 20 июля 2020 г. № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы» указано, что «оператор финансовой платформы должен иметь на праве собственности или ином законном основании основной и резервный комплексы программно-аппаратных средств...»<sup>8</sup>. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»<sup>9</sup> дополнен с 1 ноября 2017 г. статьёй 15.8, которая использует термин «программно-аппаратные

---

<sup>3</sup> Матыцин Д. Е. Дистанционные инвестиционные сделки: регулирование взаимных интересов и защита прав участников: дис. ... д-ра юрид. наук. Волгоград, 2023. 386 с.

<sup>4</sup> Николаев И. Правовая охрана и гражданско-правовой оборот прав на результаты интеллектуальной деятельности, входящие в сложный объект // Интеллектуальная собственность. Промышленная собственность. 2016. № 6. С. 34.

<sup>5</sup> Кузнецов П. У. Концептуальные условия государственной политики в сфере цифровой трансформации общества // Российское право: образование, практика, наука. 2018. № 6 (108). С. 16.

<sup>6</sup> Андреева Е. М. Некоторые компоненты выпуска и оборота цифровых валют в Российской Федерации // Банковское право. 2023. № 1. С. 12–18. DOI 10.18572/1812-3945-2023-1-12-18.

<sup>7</sup> Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (с изм. и доп.) // СПС «КонсультантПлюс». URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_220885/](https://www.consultant.ru/document/cons_doc_LAW_220885/) (дата обращения: 19.05.2024).

<sup>8</sup> Федеральный закон от 20 июля 2020 г. № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы» (с изм. и доп.) // СПС «КонсультантПлюс». URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_357765/](https://www.consultant.ru/document/cons_doc_LAW_357765/) (дата обращения: 19.05.2024).

<sup>9</sup> Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп.) // СПС «КонсультантПлюс». URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](https://www.consultant.ru/document/cons_doc_LAW_61798/) (дата обращения: 19.05.2024).

средства доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен»<sup>10</sup>.

Д. А. Казанцев называет искусственный интеллект программно-аппаратным комплексом<sup>11</sup>. К. К. Таран указывает, что облачное хранилище информации является программно-аппаратным комплексом<sup>12</sup>. А. А. Карцхия даёт определение цифровых платформ как совокупности программно-аппаратных комплексов<sup>13</sup>. Е. М. Стырин и Н. Е. Дмитриева также квалифицируют цифровую платформу как «технологический программно-аппаратный комплекс»<sup>14</sup>. Во всех этих работах указанное понятие не раскрывается и не исследуется.

Таким образом, можно сделать вывод, что несмотря на использование термина «программно-аппаратный комплекс», его исследованию и выявлению правового режима не уделяется внимания.

Согласно легальной дефиниции программно-аппаратный комплекс – это «комплекс технических и программных средств (программного обеспечения), работающих совместно для выполнения одной или нескольких специальных задач, являющийся электронной вычислительной машиной или специализированным электронным устройством (устройствами), функционально-технические характеристики которого (которых) определяются исключительно совокупностью программного обеспечения и технических средств и не могут быть реализованы при их разделении. Программно-аппаратный комплекс является самостоятельно используемым, законченным техническим изделием, имеющим серийный номер» (п. 2 Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации<sup>15</sup>).

Классификатор программно-аппаратных комплексов, утв. Приказом Министерства цифрового развития, связи и мировых коммуникаций РФ от 31 января 2023 г. № 62, приводит примеры таких комплексов: программно-

---

<sup>10</sup> Федеральный закон от 29 июля 2017 г. № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». URL:

[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_221230/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100009](https://www.consultant.ru/document/cons_doc_LAW_221230/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100009) (дата обращения: 19.05.2024).

<sup>11</sup> Казанцев Д. А. Проблемы и перспективы регулирования отношений в рамках сделки, совершенной с участием искусственного интеллекта // Journal of Digital Technologies and Law. 2023. № 1(2). С. 438–463. DOI: 10.21202/jdtl.2023.18.

<sup>12</sup> Таран К. К. Правовой режим хранения информации в облачном хранилище: дис. ... канд. юрид. наук. М., 2023. С. 33, 176.

<sup>13</sup> Карцхия А. А. Гражданско-правовая модель регулирования цифровых технологий: дис. ... д-ра юрид. наук. М., 2019. С. 213.

<sup>14</sup> Государственные цифровые платформы: формирование и развитие / Е. М. Стырин, Н. Е. Дмитриева; Нац. исслед. ун-т «Высшая школа экономики». М.: Изд. дом Высшей школы экономики, 2021. 192 с.

<sup>15</sup> Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (с изм. и доп.) // СПС «Гарант». URL: <https://base.garant.ru/71252170/> (дата обращения: 13.05.2024).

аппаратные комплексы системы хранения данных, интеллектуального анализа данных (Data Mining), обработки, анализа и распознавания изображений, обработки больших данных (BigData), обеспечения облачных и распределённых вычислений, комплексы для искусственного интеллекта и другие<sup>16</sup>.

Понятие «программно-аппаратного комплекса», как отмечают специалисты, давно существует на рынке<sup>17</sup>. Определение схожей категории (программно-аппаратного средства) было дано в государственном (1993) и международных (1991, 2001) стандартах (тексты их идентичны): это «технические средства, содержащие компьютерную программу и данные, которые не могут изменяться средствами пользователя. Компьютерная программа и данные, входящие в программно-аппаратные средства, классифицируются как программное обеспечение; схемы, содержащие компьютерную программу и данные, классифицируются как технические средства»<sup>18</sup>. В профессиональных стандартах ИТ-специалистов упоминаются аппаратно-программные средства<sup>19</sup>.

Итак, программно-аппаратные комплексы представляют собой сложный объект, неразрывное сочетание программного обеспечения (нематериального компонента) и технических средств (материального компонента), причём характеристики этого объекта в целом определяются именно совокупностью элементов. Такие объекты исследуются в научной литературе, в основном посвящённой объектам гражданских правоотношений, т. к. именно в Гражданском кодексе РФ дан перечень объектов гражданских прав с чётким различием вещей и результатов интеллектуальной деятельности, к которым относятся программы для ЭВМ. Представляется, что уже давно назрела

---

<sup>16</sup> Приказ Министерства цифрового развития, связи и мировых коммуникаций РФ от 31 января 2023 г. № 62 «Об утверждении классификатора программно-аппаратных комплексов и Правил применения классификатора программно-аппаратных комплексов» (с изм. и доп.) // СПС «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/406637015/> (дата обращения: 13.05.2024).

<sup>17</sup> Российские программно-аппаратные комплексы: новый виток развития: обзор TAdviser // TAdviser: Государство. Бизнес. Технологии [Электронный ресурс]. 20 октября 2023. URL: [Российские программно-аппаратные комплексы: новый виток развития \(tadviser.ru\)](https://tadviser.ru/) (дата обращения: 19.05.2024).

<sup>18</sup> Международный стандарт ИСО/МЭК 9126:1991 «Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению» (ISO/IEC 9126:1991 «Information technology. Software product evaluation. Quality characteristics and guidelines for their use») (в настоящее время заменён более новыми стандартами); Государственный стандарт Российской Федерации «Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению. Information technology. Software product evaluation. Quality characteristics and guidelines for their use. ГОСТ Р ИСО/МЭК 9126-93, утв. Постановлением Госстандарта РФ от 28 декабря 1993 г. № 267 // Электронный фонд правовых и нормативно-технических документов. URL: <https://docs.cntd.ru/document/1200009076> (дата обращения: 19.05.2024); ГОСТ ИСО/МЭК 9126-2001. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению. Принят Евразийским Советом по стандартизации, метрологии и сертификации (протокол № 20 от 2 ноября 2001 г.) // <https://files.stroyinf.ru/Data/701/70141.pdf> (дата обращения: 19.05.2024).

<sup>19</sup> Приказ Минтруда России от 04 октября 2022. № 613н «Об утверждении профессионального стандарта «Специалист в области аппаратно-программных средств цифровой обработки сигналов»; зарегистрирован в Минюсте России 08 ноября 2022 № 70864 // СПС «КонсультантПлюс». URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_431027/65005c1c080c56529b61a1722b9b7b289e280d6c/](https://www.consultant.ru/document/cons_doc_LAW_431027/65005c1c080c56529b61a1722b9b7b289e280d6c/) (дата обращения: 19.05.2024).



потребность включения в этот перечень сложных объектов, представляющих сочетание ныне предусмотренных в ГК объектов, в результате которого целое приобретает новые свойства, особую функциональность. Иными словами, характеристики всего комплекса как системы элементов не равны набору характеристик элементов, составляющих эту систему.

Рассмотрим элементы правового режима программно-аппаратных комплексов, сформировавшегося в течение полутора последних лет, хотя данный режим и не охватывает всех аспектов отношений по поводу создания и функционирования таких объектов. Его формирование имеет, прежде всего, публично-правовые цели, такие, как охрана информационной и иной безопасности государства, обеспечение импортозамещения, поддержка отечественных производителей программно-аппаратных комплексов.

Введены меры, направленные на обеспечение технологической независимости и безопасности критической информационной инфраструктуры. В частности, Указом Президента РФ № 166 от 30 марта 2022 г. «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»<sup>20</sup> заказчики, осуществляющие закупки в соответствии с Федеральным законом № 223-ФЗ, с 31 марта 2022 г. не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов без согласования с федеральным органом исполнительной власти, уполномоченным Правительством РФ, а с 1 января 2025 г. органам государственной власти и заказчикам, осуществляющим закупки по указанному закону, запрещается использовать иностранное ПО на принадлежащих им значимых объектах критической информационной инфраструктуры.

Были приняты Требования к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (далее – заказчики), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, Правила согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками и Правила перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, заказчиками, на принадлежащих им значимых объектах критической информационной инфраструктуры (утверждены Постановлением Правительства РФ от 22 августа 2022 г. № 1478<sup>21</sup>).

---

<sup>20</sup> Указ Президента РФ № 166 от 30 марта 2022 г. «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» // СПС «Гарант». URL: <https://ivo.garant.ru/#/document/403784114/paragraph/1:0> (дата обращения: 19.05.2024).

<sup>21</sup> Постановление Правительства РФ от 22 августа 2022 г. № 1478 «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов,

В конце 2022 г. были внесены изменения в Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации<sup>22</sup>, а также введены Требования к техническим средствам в составе программно-аппаратного комплекса для включения в единый реестр российских программ для электронных вычислительных машин и баз данных<sup>23</sup>. Они предусматривают возможность включения в единый реестр российских программ для электронных вычислительных машин и баз данных программно-аппаратных комплексов. Включение в указанный реестр имеет последствия в виде предоставления производителям этих комплексов определённых преимуществ (льгот по налогу на прибыль, согласно Налоговому кодексу РФ, выделения государственных субсидий для поддержки отечественных производителей в ИТ-сфере).

Были разработаны Классификатор программно-аппаратных комплексов и Правила применения классификатора программно-аппаратных комплексов, они утверждены Приказом Министерства цифрового развития, связи и мировых коммуникаций РФ от 31 января 2023 г. № 62<sup>24</sup>. Эти акты используются в целях обеспечения ведения единого реестра российских программ для электронных вычислительных машин и баз данных.

---

используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, правил согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, а также закупок услуг, необходимых для использования этого программного обеспечения на таких объектах, и правил перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс». URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_425279/](https://www.consultant.ru/document/cons_doc_LAW_425279/) (дата обращения: 14.05.2024).

<sup>22</sup> Постановление Правительства РФ от 28 декабря 2022 г. № 2461 «О внесении изменений в постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 и признании утратившими силу отдельных положений некоторых актов Правительства Российской Федерации» // СПС «Гарант». URL: [https://base.garant.ru/406060493/#block\\_1021](https://base.garant.ru/406060493/#block_1021) (дата обращения: 13.05.2024).

<sup>23</sup> Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (с изм. и доп.) // СПС «Гарант». URL: <https://base.garant.ru/71252170/> (дата обращения: 13.05.2024).

<sup>24</sup> Приказ Министерства цифрового развития, связи и мировых коммуникаций РФ от 31 января 2023 г. № 62 «Об утверждении классификатора программно-аппаратных комплексов и Правил применения классификатора программно-аппаратных комплексов» (с изм. и доп.) // СПС «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/406637015/> (дата обращения: 13.05.2024).

Последними были приняты Правила перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации (утверждены Постановлением Правительства РФ от 14 ноября 2023 г. № 1912, вступают в действие 1 сентября 2024 г. и действуют до 1 сентября 2030 г.)<sup>25</sup>.

На основании всего вышесказанного, можно сделать следующие выводы. Программно-аппаратный комплекс – это комплекс технических и программных средств, характеристики которого определяются исключительно совокупностью программного обеспечения и технических средств и не могут быть реализованы при их разделении. Их правовой режим сформирован в публично-правовой сфере с целью охраны информационной безопасности государства и осуществления импортозамещения. С точки зрения гражданского оборота эти комплексы представляют собой сложные объекты, включающие программы для ЭВМ и оборудование (вещи). Представляется необходимым введения в законодательство такой категории объектов гражданского оборота, как сложные объекты, правовой режим которых включает их неделимость. Программно-аппаратные комплексы являются примерами таких объектов.

### Список литературы

1. Андреева Е. М. Некоторые компоненты выпуска и оборота цифровых валют в Российской Федерации // Банковское право. 2023. № 1. С. 12–18. DOI: 10.18572/1812-3945-2023-1-12-18.
2. Государственные цифровые платформы: формирование и развитие / Е. М. Стырин, Н. Е. Дмитриева; Нац. исслед. ун-т «Высшая школа экономики». М.: Изд. дом Высшей школы экономики, 2021. 192 с.
3. Казанцев Д. А. Проблемы и перспективы регулирования отношений в рамках сделки, совершенной с участием искусственного интеллекта // Journal of Digital Technologies and Law. 2023. № 1 (2). С. 438–463. DOI: 10.21202/jdtl.2023.18.
4. Карцхия А. А. Гражданско-правовая модель регулирования цифровых технологий: дисс. ... д-ра юрид. наук. М., 2019. 394 с.
5. Кузнецов П. У. Концептуальные условия государственной политики в сфере цифровой трансформации общества // Российское право: образование, практика, наука. 2018. № 6 (108). С. 12–17.

---

<sup>25</sup> Постановление Правительства РФ от 14 ноября 2023 г. № 1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации» // СПС «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/407912691/> (дата обращения: 14.05.2024).

6. Матыцин Д. Е. Дистанционные инвестиционные сделки: регулирование взаимных интересов и защита прав участников: дис. ... д-ра юрид. наук. Волгоград, 2023. 386 с.

7. Николаев И. Правовая охрана и гражданско-правовой оборот прав на результаты интеллектуальной деятельности, входящие в сложный объект // Интеллектуальная собственность. Промышленная собственность. 2016. № 6. С. 33–42.

8. Таран К. К. Правовой режим хранения информации в облачном хранилище: дис. ... канд. юрид. наук. М., 2023. 237 с.

**Oksana V. Zhevnyak**

PhD (Law), Associate Professor, Associate Professor of the  
Department of Legal Regulation of Economic Activities,  
Ural Federal University named after the first President of Russia B. N. Yeltsin  
(Yekaterinburg, Russian Federation)

## **LEGAL REGIME OF SOFTWARE AND HARDWARE COMPLEXES**

**Abstract:** The article examines the concept of software and hardware systems, their legal definition, their legal regime, which includes public legal norms aimed at protecting the information security of the state and ensuring import substitution. It is concluded that software and hardware systems are complex objects, including computer programs and equipment (computers, electronic devices), and the functioning of the complex is possible only through a combination of these elements. The objective existence of such complexes, other similar complex objects and their participation in civil circulation require their reflection in the list of objects of civil rights and inclusion in their private legal regime of the sign of indivisibility.

**Keywords:** software and hardware systems, hardware and software systems, legal regime, legal regulation, complex objects.

**Зуев Сергей Васильевич**

Доктор юридических наук, профессор,  
профессор кафедры судебной и правоохранительной деятельности,  
Южно-Уральский государственный университет  
(национальный исследовательский университет)  
(г. Челябинск, Российская Федерация)  
zuevsergej@inbox.ru

## **ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЙ ПРОЦЕСС УГОЛОВНОГО СУДОПРОИЗВОДСТВА: ВОПРОС ВРЕМЕНИ**

**Аннотация:** В статье автор утверждает, что спустя некоторое время произойдёт переход на информационно-технологический процесс уголовного судопроизводства. В частности, потребуется создание цифровой платформы, объединяющей несколько модулей (кластеров) для обеспечения электронного взаимодействия всех участников уголовно-процессуальных отношений.

**Ключевые слова:** цифровизация, уголовное судопроизводство, цифровая платформа, электронное взаимодействие, информационные технологии, модули.

Трансформация уголовного судопроизводства в условиях тотальной цифровизации общества и государства не может не затронуть доктринальные, устоявшиеся основы уголовного судопроизводства – сферы деятельности, которая характеризуется как процессуальная.

Процесс – это порядок, последовательность, процедурность выполняемых действий и принятия решений в рамках конкретного уголовного дела. Развитие информационных технологий и их внедрение в уголовный процесс неизбежно приведут к переходу на электронные «рельсы» досудебного производства и рассмотрения уголовных дел в суде. Вместе с этим, привычная процессуальная сторона уголовно-процессуальной деятельности также должна подвергнуться кардинальным изменениям.

В перспективе ожидается появление и развитие информационно-технологического процесса уголовного судопроизводства, который может осуществляться в цифровой среде в порядке электронного производства по уголовным делам.

Представляется, что переход на полноценный информационно-технологический процесс должен сопровождаться кардинальными переменами, находящими отражение (правовое закрепление) в уголовно-процессуальном законодательстве, а именно:

– активное внедрение современных информационных технологий в уголовный процесс;

- разработка, использование и постоянное совершенствование цифровых модулей, а также подмодулей (или приложений) цифровой платформы электронного производства по уголовным делам;
- широкое электронное взаимодействие всех участников уголовно-процессуальных отношений;
- стирание граней между уголовно-процессуальной и оперативно-розыскной (поисковой) деятельности, осуществляемой в электронной форме;
- масштабная цифровизация судебно-экспертной деятельности;
- расширение прав и возможностей стороны защиты в плане собирания и представления доказательств в электронном виде (электронных документов, фото, аудио- и видеоматериалов);
- активное использование автоматизированных информационных систем и технологий искусственного интеллекта для решения задач цифрового уголовного судопроизводства.

Дальнейшее развитие информационных технологий в уголовном судопроизводстве создаст предпосылки для перехода на **«беспредметный» цифровой уголовный процесс**.

Привычное уголовное судопроизводство имеет сущностное выражение в виде участников правоотношений и их действий, вещественных доказательств и документов как материальных объектов. В эпоху развития цифровой трансформации общества и государства требуется общедоступная цифровая среда для осуществления уголовного судопроизводства.

«Беспредметный» цифровой уголовный процесс может включать в себя несколько самостоятельных кластеров (или модулей). В данном случае под кластером понимается подмножество результатов поиска, связанных единством темы. Если применять некую аналогию с использованием электронного уголовного дела в Республике Казахстан, то относительно самостоятельные части цифрового уголовного судопроизводства можно обозначить как модули.

**Первый модуль.** *Первичный сбор информации о преступлении.* На данном этапе предполагается широкое применение видеокамер, сканеров и другой техники, позволяющей получать с места происшествия максимально возможную электронную машиночитаемую информацию. Важный вопрос о субъекте, правомочном заниматься этой деятельностью. Представляется, что в идеале он не должен представлять интересы той или иной стороны в уголовном процессе. Его задача компетентно, грамотно собрать всю информацию и перенаправить её (загрузить) в облачное пространство цифровой платформы уголовного судопроизводства.

**Второй модуль.** *Накопление материалов электронного уголовного дела.* Цифровая платформа уголовного судопроизводства самостоятельно собирает, подгружает информацию о каждом участнике, в том числе предполагаемом лице, совершившем преступление. В данном случае автономно работают различные программы, подключаются системы и базы данных, в том числе с применением

информационной технологии OSINT<sup>1</sup>. Могут проводиться следственные действия и оперативно-розыскные мероприятия<sup>2</sup>, а также экспертизы по информации, имеющейся в деле<sup>3</sup>. По итогу готовятся два заключения: обвинительное и защитное; а также проект решения, предложенный с помощью технологий искусственного интеллекта. Участники информируются об этом и вправе согласиться с предложенным решением. В противном случае назначается дата и время рассмотрения уголовного дела в судебном заседании посредством видео-конференц-связи.

**Третий модуль.** *Дистанционное рассмотрение уголовного дела в суде.* С помощью видео-конференц-связи проводится судебное заседание. Заслушиваются участники уголовного процесса. Принимается итоговое судебное решение, которое, если отличается от предложенного с помощью технологии искусственного интеллекта, то должно быть обоснованным и мотивированным.

**Четвёртый модуль.** *Исполнение приговора.* Осуществляется обращение приговора к исполнению. Система формирует и направляет в соответствующие учреждения и организации необходимые документы посредством электронного взаимодействия. По результатам исполнения наказания соответствующие государственные органы и учреждения должны выставить электронную карточку об этом в общую информационную систему цифровой платформы уголовного судопроизводства.

**Пятый модуль.** *Обжалование решений, принятых судом.* Данный функционал предусматривает апелляционное, кассационное, надзорное обжалование, а также возможность возобновления производства по уголовным делам ввиду новых или вновь открывшихся обстоятельств. Жалобы на решения

---

<sup>1</sup> Подробнее об этом см., например: Современные возможности Главного управления криминалистики (Криминалистического центра) в сфере технико-криминалистического обеспечения расследования преступлений // Вестник Главного управления криминалистики. 2022. № 11 (80). С. 7–12; Бессонов А. А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) // Актуальные вопросы теории и практики оперативно-разыскной деятельности: Сборник научных трудов Межведомственной научно-практической конференции (Москва, 16 сентября 2022 года). Москва, 2022. С. 40–45; Бахтеев Д. В. Проблемы OSINT как источника криминалистически значимых сведений // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции: в 6 т. (Казань, 22 сентября 2023 года). Казань, 2023. С. 36–39; Яковлева К. Ю. Использование технологии OSINT в ходе обыска места нахождения электронной информации // Проблемы правовой и технической защиты информации. 2023. № 11. С. 131–136.

<sup>2</sup> Хромов И. Л., Кузьмин Н. А., Завьялов И. А. Перспективные направления использования искусственного интеллекта в оперативно-розыскной деятельности // Оперативно-розыскная деятельность в цифровом мире: сборник научных трудов / под ред. В. С. Овчинского. М., 2021. С. 94–103.

<sup>3</sup> Подробнее об этом см.: Саркисян А. А. Цифровизация судебно-экспертной деятельности: теоретические, правовые и организационные аспекты: автореф. дис. ... канд. юрид. наук. М., 2024. 24 с.

суда подаются в электронном виде. К ним могут прикрепляться различного рода документы. Рассмотрение жалоб и представлений проводится в онлайн режиме.

Количество модулей, а также подмодулей (или приложений) в итоге может несколько отличаться от предложенных. Однако в любом случае цифровая платформа уголовного судопроизводства должны быть основана на использовании электронной машиночитаемой информации, неразрывно связана с электронным взаимодействием всех участников процесса и предназначена для осуществления «беспредметного» цифрового уголовного процесса.

В перспективе проблемной видится ситуация, когда от решения организационно-технических вопросов будет напрямую зависеть соблюдение и обеспечение прав участников уголовного процесса, а значит и право на доступ к правосудию. И здесь нужно говорить о двухуровневом или даже трёхуровневом правовом регулировании.

В прошлом столетии уголовно-процессуальные отношения регулировались строго нормами уголовно-процессуального кодекса. Последний правовой акт был самодостаточен. Однако в настоящее время ситуация кардинально меняется. Ряд статей в УПК РФ имеют ссылки на действующее законодательство, например: ч. 3 ст. 1, ч. 3 ст. 11, п. в. ч. 2 ст. 82, ч. 3 ст. 118, ч. 1.3. ст. 140, ч. 1.2 ст. 148, ч. 1 ст. 161.1, ч. 4.1. ст. 164, ч. 8 ст. 208, ч. 4 ст. 213, ч. 5.1 ст. 220, ч. 3.2. ст. 225, ч. 11 ст. 226.7, ч. 5 ст. 239, п. 1 ч. 1 ст. 313.1, ч. 2 ст. 446.2, ч. 1 ст. 446.3 УПК РФ и др.

Причём просматривается явная зависимость процессуальных норм от положений других законов. К примеру, согласно ч. 3 ст. 11 УПК РФ к «защищаемым лицам» могут применять меры безопасности, предусмотренные ч. 9 ст. 166, ч. 2 ст. 186, ч. 8 ст. 193, п. 4 ч. 2 ст. 241, ч. 5 ст. 278 УПК РФ, а также «иные меры безопасности, предусмотренные законодательством Российской Федерации».

Имеются уже ссылки и на подзаконные акты. Так, в соответствии с ч. 4 ст. 474.2 УПК РФ порядок подачи прокурору, следователю, руководителю следственного органа, в орган дознания, дознавателю документов в электронном виде, а также требования к форматам ходатайства, заявления, жалобы, представления, требования и используемым техническим средствам могут определяться нормативными правовыми актами Следственного комитета Российской Федерации, федеральных органов исполнительной власти, в состав которых входят органы предварительного расследования, Генеральной прокуратуры Российской Федерации<sup>4</sup>.

Все это не что иное, как подтверждение многоуровневого правового регулирования процессуальных отношений и прямое влияние законов и подзаконных актов на производство по уголовным делам.

Все это свидетельствует о нарастающей тенденции, связанной с зависимостью решения задач уголовного судопроизводства от применения,

---

<sup>4</sup> Федеральный закон от 25.12.2023 № 672-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2023. № 297.



помимо УПК, законов и подзаконных актов. Представляется, что в цифровой среде эта закономерность только усилится.

Переход на информационно-технологический процесс уголовного судопроизводства предполагает создание соответствующей цифровой платформы для обеспечения электронного производства по уголовным делам. Дело только во времени, в решении финансовых, организационных и технических вопросов, а также в разработке научного обоснования и создании законодательной базы.

### **Список литературы**

1. Бахтеев Д. В. Проблемы OSINT как источника криминалистически значимых сведений // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции: в 6 т. (Казань, 22 сентября 2023 года). Казань, 2023. С. 36–39.

2. Бессонов А. А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) // Актуальные вопросы теории и практики оперативно-разыскной деятельности: Сборник научных трудов Межведомственной научно-практической конференции (Москва, 16 сентября 2022 года). Москва, 2022. С. 40–45.

3. Саркисян А. А. Цифровизация судебно-экспертной деятельности: теоретические, правовые и организационные аспекты: автореф. дис. ... канд. юрид. наук. М., 2024. 24 с.

4. Современные возможности Главного управления криминалистики (Криминалистического центра) в сфере технико-криминалистического обеспечения расследования преступлений // Вестник Главного управления криминалистики. 2022. № 11 (80). С. 7–12.

5. Хромов И. Л., Кузьмин Н. А., Завьялов И. А. Перспективные направления использования искусственного интеллекта в оперативно-розыскной деятельности // Оперативно-розыскная деятельность в цифровом мире: сборник научных трудов / под ред. В. С. Овчинского. М., 2021. С. 94–103.

6. Яковлева К. Ю. Использование технологии OSINT в ходе обыска места нахождения электронной информации // Проблемы правовой и технической защиты информации. 2023. № 11. С. 131–136.

**Sergey V. Zuev**

Doctor of Law, assistant professor,  
professor of the Department of Judicial and Law Enforcement Activities  
South Ural State University (national research university)  
(Chelyabinsk, Russian Federation)  
zuevsergj@inbox.ru

## **INFORMATION-TECHNOLOGICAL PROCESS OF CRIMINAL PROCEEDINGS: A MATTER OF TIME**

**Abstract:** In the article the author argues that after some time there will be a transition to the information-technological process of criminal proceedings. In particular, it will be necessary to create a digital platform that combines several modules (clusters) to ensure electronic interaction of all participants of criminal procedural relations.

**Keywords:** digitalisation, criminal proceedings, digital platform, electronic interaction, information technology, modules.

**Иванов Владислав Юрьевич**

Старший преподаватель кафедры криминалистики,  
Уральский юридический институт МВД России  
(г. Екатеринбург, Российская Федерация)  
vivanov533@mvd.ru

**Янкевич Екатерина Алексеевна**

Курсант факультета подготовки следователей,  
Уральский юридический институт МВД России  
(г. Екатеринбург, Российская Федерация)  
blad02051995@mail.ru

**ЛИЧНОСТЬ НЕСОВЕРШЕННОЛЕТНЕГО КИБЕРПРЕСТУПНИКА КАК  
ЭЛЕМЕНТ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ  
ПРЕСТУПЛЕНИЙ**

**Аннотация:** В статье рассмотрена характеристика личности несовершеннолетнего киберпреступника, совершающего противоправные деяния как единолично, так и в составе организованной группы. Авторы акцентируют внимание на поведенческих особенностях личности несовершеннолетнего преступника, анализируя которые следователь (дознатель) способен выдвигать криминалистические версии, планировать применение тактических приёмов при производстве отдельных следственных действий.

**Ключевые слова:** несовершеннолетний киберпреступник, несовершеннолетний подозреваемый, криминалистическая характеристика, криминалистические версии, детская психология, подросток, формирование личности.

Личность несовершеннолетнего преступника занимает важное место в структуре криминалистической характеристики преступлений. Изучение её с точки зрения науки криминалистики способствует пониманию причин и условий, способствующих совершению противоправных деяний. Сегодня особое внимание следует уделять несовершеннолетним лицам, совершающим преступления с использованием информационно-телекоммуникационных технологий.

В настоящее время подростки большую часть свободного времени проводят в сети Интернет, где общаются между собой, играют в онлайн игры и т. п. Вместе в этом некоторые подростки начинают увлекаться деятельностью в киберпространстве, связанную со взломом аккаунтов в социальных сетях, сбором информации из открытых источников о своих сверстниках, знакомых

известных личностей (OSINT)<sup>1</sup>. В процессе этих увлечений они находят единомышленников, как правило возрастом постарше, которые направляют их и показывают, что, обладая определёнными навыками в киберпространстве, возможно использовать свои знания в области IT-технологий не только ради шуточных увлечений над сверстниками, но и для заработка.

К сожалению, далеко не всегда несовершеннолетние лица, осуществляющие незаконные действия в информационно-телекоммуникационном пространстве, осознают общественную опасность таких действий.

Психология современных подростков такова, что люди, обладающие навыками в области IT либо хакерскими способностями, являются наиболее привлекательными для подражания. Стараясь быть похожим на них, несовершеннолетний киберпреступник чувствует себя неуязвимым и безнаказанным при совершении противоправных действий в сети Интернет.

Так же ещё одним из наиболее важных критериев преступности среди несовершеннолетних является воспитание в неполной семье. Данный критерий довольно часто встречается у правонарушителей в подростковом возрасте. Только 46 % из числа правонарушителей имеют двоих родителей, а 16 % являются сиротами, которые не имеют ни отца, ни матери<sup>2</sup>.

Одним из основных и глобальных условий преступности среди несовершеннолетних в целом следует считать так называемый духовный кризис современного поколения молодёжи: на протяжении длительного времени учёные из различных научных сфер сигнализируют о том, что наиболее значимые социальные и духовные ценности отсутствуют у молодёжи, при этом всё большую значимость и уважение среди них приобретает умаление привычных моральных и нравственных норм и правил, их повсеместное нарушение. Чем более пренебрежительное поведение подростка к окружающим, тем более уважаемым и авторитетным он становится в собственной среде (среди таких же, как он).

По этой причине таких подростков с лёгкостью заманивают в свои ряды. Они вербуют несовершеннолетних лиц по целому ряду причин: во-первых, такая вербовка крайне просто реализуема, ведь на фоне общей тенденции подростки и сами желают быть более авторитетными в связи с участием в совершении преступления, как говорилось ранее; во-вторых, уже находясь в сообществе, несовершеннолетние крайне легко поддаются влиянию, поскольку в силу незрелого возраста не могут оказать должного сопротивления даже тогда, когда не согласны с решением сообщества о совершении того или иного преступления; наконец, в-третьих (и это самый главный аспект), несовершеннолетние

---

<sup>1</sup> Дерюгин Р. А., Иванов В. Ю. Использование «разведки» по открытым источникам (OSINT) для получения криминалистически значимой информации из сети Интернет // Борьба с преступностью: теория и практика. Тезисы докладов XI Международной научно-практической конференции. Могилев, 2023. С. 426.

<sup>2</sup> Бошаева Л. Л. Криминологическая характеристика киберпреступности в отношении несовершеннолетних в России: монография. Москва: Проспект, 2023. С. 18.

становятся инструментом достижения преступных целей: не являясь субъектами конкретного преступного посягательства, подростки не будут привлечены к уголовной ответственности; но даже если они могут рассматриваться в качестве субъектов, уголовное наказание для них особое, более мягкое в сравнении с теми видами наказаний, которые предусмотрены для граждан, достигших совершеннолетия<sup>3</sup>.

Как правило, в совершение киберпреступлений вовлекаются подростки, имеющие низкий уровень социализации, устойчивой антисоциальной направленности, обладающие слабой волей или поведенческими дефектами. В большинстве случаев вовлечёнными оказываются подростки 14–18 лет, т. к. данный период является кризисным, наиболее трудным для них – они уже стремятся к свободе и праву выбора, однако ещё не имеют социального опыта, в результате чего зачастую поддаются негативному влиянию лиц, кажущихся им авторитетными<sup>4</sup>.

По этой причине, следователю (дознавателю), имея в производстве уголовное дело, возбуждённое в отношении несовершеннолетнего киберпреступника, необходимо более тщательно подходить к организации и проведению следственных действий. Зная поведенческие особенности личности несовершеннолетних киберпреступников, следователь (дознаватель) более эффективно сможет наладить контакт с задержанным лицом.

Обладая знаниями криминалистической характеристики киберпреступности среди несовершеннолетних, следователь (дознаватель) способен получить криминалистически значимую информацию ориентирующего характера, которая может быть использована для выдвижения версий, планирования конкретного следственного действия и всего расследования уголовного дела, прогнозирования возможного противодействия со стороны участников уголовного судопроизводства.

Таким образом, личность преступника имеет важное значение в структуре криминалистической характеристики преступлений, совершаемых несовершеннолетними с использованием информационно-телекоммуникационных технологий. Изучение психологических особенностей личности несовершеннолетнего киберпреступника должно являться первостепенной задачей следователя (дознавателя), поскольку данные знания будут способствовать качественному и эффективному раскрытию и расследованию преступлений, совершаемых несовершеннолетними в сети Интернет.

---

<sup>3</sup> Алёшина А. В. Предупреждение киберпреступности в отношении несовершеннолетних в информационном пространстве сети Интернет // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2022. № 8. С. 5–9.

<sup>4</sup> Федосеева О. И. Психологические особенности формирования личности несовершеннолетнего киберпреступника // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 176.

## Список литературы

1. Алёшина А. В. Предупреждение киберпреступности в отношении несовершеннолетних в информационном пространстве сети Интернет // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2022. № 8. С. 5–9.
2. Бошаева Л. Л. Криминологическая характеристика киберпреступности в отношении несовершеннолетних в России: монография. Москва: Проспект, 2023. 144 с.
3. Дерюгин Р. А., Иванов В. Ю. Использование «разведки» по открытым источникам (OSINT) для получения криминалистически значимой информации из сети Интернет // Борьба с преступностью: теория и практика. Тезисы докладов XI Международной научно-практической конференции. Могилев, 2023. С. 424–428.
4. Федосеева О. И. Психологические особенности формирования личности несовершеннолетнего киберпреступника // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 174–178.

**Vladislav Yu. Ivanov**

Senior Lecturer of the Department of Forensic Science,  
Ural Law Institute of the Ministry of Internal Affairs of Russia  
(Yekaterinburg, Russian Federation)  
vivanov533@mvd.ru

**Ekaterina A. Yankevich**

Student,  
Ural Law Institute of the Ministry of Internal Affairs of Russia  
(Yekaterinburg, Russian Federation)  
blad02051995@mail.ru

## IDENTITY OF A JUVENILE CYBER CRIMINAL AS AN ELEMENT OF FORENSIC CHARACTERISTICS OF CRIMES

**Abstract:** The article examines the personality characteristics of a minor cybercriminal who commits illegal acts, both individually and as part of an organized group. The authors focus on the behavioral characteristics of the personality of a minor offender, by analyzing which the investigator (interrogator) is able to put forward forensic versions and plan the use of tactics in the performance of individual investigative actions.

**Keywords:** juvenile cybercriminal, juvenile suspect, forensic characteristics, forensic versions, child psychology, teenager, personality formation.

**Каравая Анастасия Владимировна**

Старший преподаватель кафедры «Безопасность в цифровом мире»,  
Московский государственный технический университет имени Н. Э. Баумана  
(национальный исследовательский университет)  
Аспирант кафедры уголовного права, уголовного процесса и криминалистики,  
Государственный университет просвещения  
(г. Москва, Российская Федерация)  
karlova\_av@bmstu.ru

## **ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ПРИМЕНЕНИЯ ИТ-ТЕХНОЛОГИЙ В СИСТЕМЕ ПРОФИЛАКТИКИ ПРЕСТУПЛЕНИЙ**

**Аннотация:** Статья посвящена теоретико-правовым основам применения ИТ-технологий в системе профилактики преступлений. Вопросы профилактики преступлений занимают важное место в системе криминологии, поскольку выявление и устранение причин и условий совершения преступлений является одной из приоритетных задач современного общества. В статье описывается правовая регламентация использования ИТ-технологий в системе профилактики преступлений с позиций Федерального закона от 23.06.2016 № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации». В статье рассматривается, что развитие ИТ-технологий предоставляет новые возможности для улучшения процессов профилактики и борьбы с преступлениями. Это обусловлено возможностью эффективного сбора, хранения, обработки и анализа данных, а также созданием инновационных инструментов для превентивных мер и оперативного реагирования на угрозы. Исходя из этого, можно отметить, что субъекты системы профилактики не все направления реализуют с помощью ИТ-технологий. Это открывает новое направление – профилактика преступлений с помощью ИТ-технологий.

**Ключевые слова:** ИТ-технологии, информационные технологии, профилактика преступлений, система профилактики преступлений, преступления.

В современном правовом государстве профилактика преступлений является одним из наиболее эффективных способов борьбы с преступностью. Любое преступление независимо от тяжести совершённого деяния наносит ущерб общественным интересам и ключевым ценностям социума. Экономические затраты государства с высоким уровнем преступности несопоставимы с уровнем затрат государства, в котором уровень преступной активности находится в пределах общепринятой нормы. Однако ущерб от преступной деятельности исчисляется не только финансовыми потерями, но и

жизнями людей<sup>1</sup>. «Разгул» преступности провоцирует рост социальной напряжённости в обществе, а также общую неудовлетворенность социума правовой и карательной политикой государства.

Негативные последствия для экономики, рост социальной напряжённости, формирование прослойки общества, для которой преступное поведение является нормой жизни и способом заработка, все это является прямым следствием преступной деятельности<sup>2</sup>.

В частности, глобальная информатизация мирового сообщества и развитие компьютерной сети Интернет привели к тому, что информационно-телекоммуникационные инфраструктуры оказались весьма уязвимыми объектами воздействия. В свете быстрого развития цифровой сферы компьютерные преступления стали значительной угрозой для нашего общества в целом и личной безопасности граждан. Рост таких преступлений вызывает необходимость действий со стороны компетентных лиц.

Продолжая мысль, можно сказать, что на данный момент любой традиционный вид преступления можно «модернизировать», используя информационные технологии (далее – ИТ-технологии), что представляет некоторые сложности не только для раскрытия и расследования преступлений, но и для их профилактики.

Однако прежде, чем непосредственно перейти к рассмотрению вопросов такой профилактики, необходимо остановиться на отдельных общих аспектах. Так, в статье 2 Федерального закона от 23.06.2016 № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» (далее – ФЗ №182) закреплены понятия, которые используются для его целей: «профилактика правонарушений» – совокупность мер социального, правового, организационного, информационного и иного характера, направленных на выявление и устранение причин и условий, способствующих совершению правонарушений, а также на оказание воспитательного воздействия на лиц в целях недопущения совершения правонарушений или антиобщественного поведения и «система профилактики правонарушений» – совокупность субъектов профилактики правонарушений, лиц, участвующих в профилактике правонарушений, и принимаемых ими мер профилактики правонарушений, а также основ координации деятельности и мониторинга в сфере профилактики правонарушений<sup>3</sup>.

Вместе с тем, использование ИТ-технологий для реализации функций субъектов профилактики не регламентировано ФЗ №182. Исходя из этого,

---

<sup>1</sup> Новицкий А. А. Профилактика преступлений в Российской Федерации // Скиф. Вопросы студенческой науки. 2020. № 11 (51). С. 276–279.

<sup>2</sup> Новицкий А. А. Профилактика преступлений в Российской Федерации // Скиф. Вопросы студенческой науки. 2020. № 11 (51). С. 276–279.

<sup>3</sup> Федеральный закон «Об основах системы профилактики правонарушений в Российской Федерации» от 23.06.2016 N 182-ФЗ // КонсультантПлюс [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_199976/](https://www.consultant.ru/document/cons_doc_LAW_199976/) (дата обращения: 11.05.2024).



открывается большое поле усовершенствования системы профилактики преступлений с помощью ИТ-технологий.

Интеграция ИТ-технологий в профилактику преступлений играет важную роль в современном обществе, поскольку позволяет использовать передовые технологии и аналитические инструменты.

Теоретические основы интеграции ИТ-технологий в профилактику преступлений основываются на предположении о том, что использование передовых информационно-технических средств позволяет значительно улучшить эффективность профилактической деятельности. Такие технологии могут помочь в обнаружении и анализе преступлений, позволяя правоохранным органам оперативно получать информацию, проводить сложный анализ данных и принимать обоснованные оперативные решения.

Возможности интеграции ИТ-технологий в профилактику преступлений огромны. Одной из них является использование аналитических инструментов для обработки больших массивов данных и выявления зависимостей между преступлениями. Это помогает разработать эффективные стратегии предотвращения и борьбы с преступностью, основанные на фактических данных.

Также стоит указать на использование систем распознавания лиц и автоматического распознавания номерных знаков. Эти технологии позволяют оперативно идентифицировать потенциальных преступников и следить за движением транспортных средств, что улучшает возможности правоохранных органов в пресечении преступлений.

Однако, важно соблюдать принципы прозрачности и справедливости при использовании ИТ-технологий в профилактике преступлений. Правоохранительные органы должны обеспечивать права граждан и соблюдать законодательство. Также необходимо учитывать возможность злоупотребления и неправомерного использования технологий, поэтому разработка соответствующих правовых механизмов и контроль за их выполнением являются неотъемлемой частью интеграции ИТ-технологий в профилактику преступлений.

Кроме того, важно развивать сотрудничество между правоохранными органами и представителями ИТ-сектора, так как это поможет эффективно применять передовые разработки в борьбе с преступностью.

Эффективность предупредительных мер может достигаться только в случаях органичного взаимодействия государственных органов с органами местного самоуправления, средствами массовой информации, образовательными организациями и гражданами, с учётом специфики деятельности каждого субъекта, заинтересованного в реализации превентивных мер<sup>4</sup>.

---

<sup>4</sup> Назмеева Л. Р. Цифровая трансформация экономики: влияние на преступность и проблемы ее предупреждения // Вестник Казанского юридического института МВД России. 2020. Т. 11. № 1 (39). С.

В целом, интеграция IT-технологий в профилактику преступлений является важным направлением развития правоохранительной системы. Она позволяет использовать передовые инструменты для повышения эффективности работы правоохранительных органов и обеспечения безопасности общества. Однако при этом необходимо соблюдать права и свободы граждан, а также законодательные нормы, чтобы предотвратить возможные негативные последствия.

### Список литературы

1. Назмеева Л. Р. Цифровая трансформация экономики: влияние на преступность и проблемы ее предупреждения // Вестник Казанского юридического института МВД России. 2020. Т. 11. № 1 (39). С. 69–74.
2. Новицкий А. А. Профилактика преступлений в Российской Федерации // Скиф. Вопросы студенческой науки. 2020. № 11 (51). С. 276–279.

**Anastasia V. Karavaeva**

Senior Lecturer, Department of «Security in the Digital World»,  
Bauman Moscow State Technical University  
Postgraduate student of the Department of  
Criminal Law, Criminal Procedure and Criminology,  
Federal State University of Education  
(Moscow, Russian Federation)  
karlova\_av@bmstu.ru

### THEORETICAL AND LEGAL BASIS OF THE APPLICATION OF IT- TECHNOLOGIES IN THE CRIME PREVENTION SYSTEM

**Abstract:** the article is devoted to the theoretical and legal foundations of the use of IT technologies in the crime prevention system. Issues of crime prevention occupy an important place in the system of criminology, since identifying and eliminating the causes and conditions for committing crimes is one of the priorities of modern society. The article describes the legal regulation of the use of IT technologies in the crime prevention system from the standpoint of Federal Law dated June 23, 2016 N 182-FZ «On the fundamentals of the crime prevention system in the Russian Federation». The article discusses that the development of IT technologies provides new opportunities for improving the processes of preventing and combating crimes. This is due to the ability to effectively collect, store, process and analyze data, as well as the creation of innovative tools for preventive measures and rapid response to threats. Based on this, it can be noted that the subjects of the prevention system do not implement all areas using IT technologies. This opens up a new direction - crime prevention using IT technologies.

**Keywords:** IT-technologies, information technologies, crime prevention, crime prevention system, crimes.

**Коваленко Наталья Евгеньевна**

Аспирант,

Юридический институт Алтайского государственного университета

(г. Барнаул, Российская Федерация)

Kovalenkorub5@gmail.com

## **ВЫЗОВЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ СОВРЕМЕННОСТИ КАК ФАКТОР РАЗВИТИЯ ПРАВОВЫХ КАТЕГОРИЙ: НА ПРИМЕРЕ СУБЪЕКТА ПРАВА**

**Аннотация:** В современных реалиях информационного общества представляется важным совершенствовать механизм правового регулирования, что невозможно без исследования истории становления фундаментальных правовых категорий, которые планируется подвергнуть обновлению. Статья посвящена анализу концепций субъекта права, изложенных учёными-правоведами в различные исторические периоды, в контексте их дальнейшей трансформации в информационных отношениях. Автор рассматривает возможность признать роботов и иные автономные системы участниками правоотношений как одну из стадий формирования комплексной теории «субъект информационного общества».

**Ключевые слова:** субъект права, правосубъектность, правоотношение, теория субъектности, информационное общество, робот.

Стремительное развитие цифровых технологий существенно меняет правовой ландшафт. Эта трансформация охватывает различные аспекты, в том числе способ доступа к юридической информации, принципы международного права, категоризацию цифрового права, а также юридическую коммуникацию и подходы к определению субъектов права.

Эволюция права в цифровом обществе затрагивает сложные онтологические и эпистемологические проблемы, включая отношения между реальным и виртуальным, а также роль искусственного интеллекта как возможного субъекта права<sup>1</sup>. В. В. Архипов указывает на проблему субъектности как главный вектор современной доктрины, способный дать ответ на правовое регулирование информационных отношений с использованием технологий искусственного интеллекта (ИИ). Так, в настоящее время идут дискуссии об определении субъектности иных участников информационных отношений. Ю. Гаврилова упоминает о роботах и автономных организациях, которые обладают интеллектом, похожим на человеческий. Если признать названные категории

---

<sup>1</sup> Гаврилова Ю. А. Проблема значения права в цифровом обществе // Юридический журнал РУДН. 2020. Т. 24. № 3. С. 608–628. DOI: 10.22363/2313-2337-2020-24-3-608-628; Архипов В. В. Субъектность как основная научная проблема «цифрового права»: развитие гипотезы // Юридический мир. 2023. № 4. С. 14–18.

субъектами, то произойдёт «деконструкция права», прежде всего потому, что категория субъект права изначально строилась, основываясь на человеке, его когнитивных и эмоциональных особенностях, а также на основе его роли в правовой системе. Чтобы избежать подобных дискуссий о роли ИИ в правоотношении, наделении его возможностью стать участником названных отношений следует понять, что представляет собой субъект права как категория.

В начале XX века, в период зарождения новых взглядов в доктрине права, появились первые учения о субъекте права, но не как отдельная теория субъектности, а в рамках теории правоотношения, психологической теории, в учениях о правосознании и других. Приведём несколько позиций относительно правового положения субъекта права. Так, Гессен упоминает, что «государство и индивид осуществляют свои интересы в пределах права, при этом они являются правовыми субъектами в одинаковом смысле»<sup>2</sup>. Н. Н. Дебольский в своей работе пишет «о физических лицах в противовес юридическим», то есть понятие физического и юридического лица стало закрепляться в доктрине, но на тот момент ещё не вошло в традицию<sup>3</sup>. С. В. Пахман упоминал о важности роли личности в праве, он отождествлял субъекта права с личностью<sup>4</sup>.

Указанные концепции не претерпели существенного изменения к настоящему времени: так, субъект права всё ещё мыслиться как лицо, наделённое автономной волей и способное самостоятельно претерпевать благоприятные или негативные последствия своего поведения. Эмоционально-волевые детерминаты сегодня выступают ключевым фактором при реализации своего статуса в правовой системе. В этой связи говорить о признании автоматизированных роботов, функционирующих на основе технологии ИИ, субъектами права пока явно преждевременно, так как их когнитивные установки и эмоциональные реакции не выявляются. При этом нельзя недооценивать развитие информационных отношений и искусственных интеллектуальных систем.

Представляется, что в условиях развития технологического прогресса, значительных автоматизации и роботизации всех форм деятельности, необходимо защитить человека как субъекта права от нарушений его прав и обязанностей. Исторический путь становления категории субъект права показал, что в начале XX в. теория о субъекте права как отдельной категории была на этапе своего зарождения, однако случившиеся переломы в государственно-правовом регулировании страны, гражданская война, отодвинули начатые процессы.

Считаем, что в настоящее время особо важно уделить внимание созданию комплексной теории субъектности, что позволит создать необходимые

---

<sup>2</sup> Гессен В. М. Административное право: популярные лекции для самообразования. Санкт-Петербург: паровая скоропеч. Г. Пожарова, 1903. С. 21.

<sup>3</sup> Гессен В. М. Административное право: популярные лекции для самообразования. Санкт-Петербург: паровая скоропеч. Г. Пожарова, 1903. С. 30–31.

<sup>4</sup> Пахман С. В. О значении личности в области гражданского права Санкт-Петербург: Типография Правительствующего Сената, 1883. 32 с.

рекомендации по усовершенствованию правового регулирования в условиях активного развития цифровых технологий.

### Список литературы

1. Архипов В. В. Субъектность как основная научная проблема «цифрового права»: развитие гипотезы // Юридический мир. 2023. № 4. С. 14–18.
2. Гаврилова Ю. А. Проблема значения права в цифровом обществе // Юридический журнал РУДН. 2020. Т. 24. № 3. С. 608–628. DOI: 10.22363/2313-2337-2020-24-3-608-628
3. Гессен В. М. Административное право: популярные лекции для самообразования. Санкт-Петербург: паровая скоропеч. Г. Пожарова, 1903. 240 с.
4. Пахман С. В. О значении личности в области гражданского права Санкт-Петербург: Типография Правительствующего Сената, 1883. 32 с.

**Natalia E. Kovalenko**

Postgraduate student,  
Law Institute of the Altai State University  
(Barnaul, Russian Federation)  
Kovalenkorub5@gmail.com

### CHALLENGES OF MODERN INFORMATION RELATIONS AS A FACTOR IN THE DEVELOPMENT OF LEGAL CATEGORIES: ON THE EXAMPLE OF A SUBJECT OF LAW

**Abstract:** In the modern realities of the information society, it seems important to improve the mechanism of legal regulation, which is impossible without studying the history of the formation of fundamental legal categories that are planned to be updated. The article is devoted to the analysis of the concepts of the subject of law, set forth by legal scholars in various historical periods, in the context of their further transformation in information relations. The author considers the possibility of recognizing robots and other autonomous systems as participants in legal relations as one of the stages of the formation of a comprehensive theory of the «subject of information society».

**Keywords:** subject of law, legal personality, legal relationship, theory of subjectivity, information society, robot.

**Леднёв Илья Валерьевич**

Аспирант кафедры криминалистики

Уральский государственный юридический университет имени В. Ф. Яковлева  
(г. Екатеринбург, Российская Федерация)

ilialednev@mail.ru

## **ПРОБЛЕМЫ УЧЁТА ПО МЕХАНИЗМУ ПРЕСТУПЛЕНИЯ\***

**Аннотация:** Залогом успешного раскрытия любых серийных преступлений выступает своевременное выявление их серийного характера сотрудниками правоохранительных органов. Важную роль в этом играют различные криминалистические учёты, в особенности – учёт по механизму совершённого преступления как наиболее универсальный. К сожалению, в настоящее время в России такого рода учёт отсутствует. В рамках настоящей статьи автор рассматривает ряд проблем, которые в обязательном порядке требуют решения в ходе разработки и введения в эксплуатацию такого учёта.

**Ключевые слова:** серийные преступления, механизм преступления, криминалистический учёт, криминалистическая регистрация.

Одной из ключевых задач, решаемых в процессе раскрытия любых серийных преступлений, выступает выявление серийности, т. е. установление того, что одно или несколько преступлений принадлежат к единой серии.

С практической точки зрения, решение этой задачи сопряжено с целым рядом трудностей: дефицит криминалистической информации о преступлении и личности преступника; временной и пространственный разрывы между преступлениями (т. е. совершение преступлений в разных местах, с временным интервалом); вариативность способов совершения преступлений и механизмов слеодообразования (определяемых как объективными, так и субъективными факторами); распределённость источников информации о преступлениях в различных делах и иных документах и т. д.

Как можно заметить, большая часть этих сложностей носит информационный характер, т. е. связана с неспособностью правоохранительных органов достаточно эффективно собирать, хранить, обрабатывать и использовать информацию, полученную в ходе деятельности по раскрытию и расследованию преступлений и охране общественного порядка.

Во всём мире (в т. ч. и в России) одним из основных направлений решения проблем информационной недостаточности выступает разработка и создание криминалистических учётов, которые представляют собой «информационно-поисковые системы правового характера, содержащие массив криминалистической информации, преобразованной специалистами при

---

\* Исследование выполнено за счет гранта Российского научного фонда № 23-78-10011, <https://rscf.ru/project/23-78-10011/>.

помощи научно-обоснованных средств и методов в целях её использования в раскрытии, расследовании и предупреждении преступлений»<sup>1</sup>.

В современной России существует большое количество таких учётов, которые могут быть классифицированы по различным основаниям:

- уровню (федеральные, региональные, местные);
- функционалу (оперативно-справочные, розыскные, экспертно-криминалистические);
- объектам учёта (учёт лиц, следов пальцев рук, орудий, предметов и т. д.);
- способам фиксации информации (описательная, фотографическая, коллекционная и т. д.),
- форме хранения информации (картотечная, журнальная, коллекционная, в виде баз данных) и т. д.

Традиционно считается, что самыми эффективными, для решения задач выявления серийности, являются такие учёты, которые содержат информацию о следах, отражающих неименные особенности преступника (например, о следах пальцев его рук, его ДНК и т. п.). Между тем, их эффективность в действительности весьма ограничена.

Так, чтобы воспользоваться подобным учётом, необходимо, чтобы упомянутые следы присутствовали на месте происшествия, были обнаружены в ходе следственных действий, находились в состоянии, пригодном для последующего исследования, были правильно зафиксированы и изъяты (т. е. без утраты идентификационных свойств), направлены на исследование, которое должно быть проведено без ошибок, после чего адекватно закодированы (т. е. внесены в соответствующую базу данных с правильным описанием идентификационных свойств) и впоследствии обнаружены там. Причём в связи с особенностями серийных преступлений, такая сложная процедура должна быть соблюдена в отношении каждого эпизода серии.

Очевидно, что на практике такое возможно далеко не всегда, что подтверждается результатами соответствующих исследований.

Так, по данным А. А. Бессонова и А. А. Гайворонской, полученным на основе исследования 1300 уголовных дел о преступлениях против личности, биологические следы были обнаружены лишь в 21 % дел, следы рук и ног – лишь в 1 %<sup>2</sup>.

В связи с этим, достаточно актуальной является задача разработки учёта, который будет содержать в себе криминалистически значимую информацию о механизмах совершённых преступлений. Такого рода учёт, по сравнению с ранее упомянутыми, будет обладать рядом преимуществ, ключевое из которых

---

<sup>1</sup> Усманов Р. А. Теория и практика использования криминалистической информации в процессе раскрытия и расследования преступлений: монография. Челябинск: Челябинский юридический ин-т МВД России, 2006. С. 119.

<sup>2</sup> Бессонов А. А., Гайворонская А. А. Прайминг и его эффекты в получении криминалистически значимой информации // Вестник Томского государственного университета. 2021. № 466. С. 207.

заклучается в его большей универсальности: даже в ситуациях, когда отсутствует следы преступления, которые непосредственно указывают на неизменные особенности преступника, сотрудники правоохранительных органов, как правило, обладают информацией либо о механизме преступления в целом, либо об отдельных его элементах (например, о месте и времени совершения преступления или его способе).

Помимо этого, такой учёт может использоваться как эмпирическая база для производства научно-криминалистических исследований и разработки рекомендаций по расследованию преступлений (в случае предоставления учёным доступа к такой базе данных), как это практикуется, например в Великобритании<sup>3</sup>.

Следует отметить, что изложенные выше тезисы не являются новыми. Так, первый учёт по механизму преступлений был разработан ещё в начале XX века в Великобритании и получил название: «Modus Operandi system». Он содержал в буквенно-цифровой форме сведения о типе преступления, преступнике, предмете посягательства, времени и месте совершения преступления, его способе и т. д.<sup>4</sup>

В настоящее время, наиболее известным аналогом «Modus Operandi system», является ViCLAS (Violent Crimes Linkage Analysis System) – криминалистический учёт в форме компьютерной базы данных, в котором содержится широкий спектр криминалистически значимой информации о различных элементах механизмов убийств и преступлений на сексуальной почве. Он был разработан в 90-ые годы прошлого столетия в Канаде<sup>5</sup>. Об эффективности ViCLAS говорит, в частности, тот факт, что помимо Канады этот учёт используется так же в Великобритании, Франции, Германии, Чехии и ряде других стран<sup>6</sup>.

Попытки создания аналогичных систем предпринимались и в России. Так, В 1990-е гг. на базе ВНИИ МВД велась разработка автоматизированной информационно-поисковой системы «Монстр», однако она так и не была реализована, и сегодня разработки в данной области прекращены<sup>7</sup>. Между тем, потребность в создании подобных систем крайне велика, о чём ещё в 2017 году

---

<sup>3</sup> Woodhams J., Davies, K., Galambos, S., Webb M. A Descriptive Analysis of the Temporal and Geographical Proximities Seen Within UK Series of Sex Offenses // Journal of Police and Criminal Psychology. 2021. Vol. 36. P. 709.

<sup>4</sup> Fosdick R. B. The Modus Operandi System in the Detection of Criminals // Journal of the American Institute of Criminal Law and Criminology. 1915. Vol. 6. № 4.

<sup>5</sup> Collins P. I., Johnson G. F., Choy A., Davidson K. T., Mackay R. E., Advances in violent crime analysis and law enforcement: The canadian violent crime linkage analysis system // Journal of Government Information. 1998. Vol. 25. № 3. P. 279.

<sup>6</sup> Violent Crime Linkage Analysis System // Royal Canadian Mounted Police [Electronic resource]. URL: <https://www.rcmp-grc.gc.ca/en/violent-crime-linkage-analysis-system> (accessed: 20.05.2024).

<sup>7</sup> Исаева Л. М. Психолого-криминалистическое портретирование: монография. М.: ФГКУ ВНИИ МВД России, 2015. С. 62.



говорил заместитель руководителя Главного управления криминалистики СК РФ А. И. Созонов<sup>8</sup>.

Итак, на основании вышеизложенного, можно убедиться, что разработка систем криминалистической регистрации на основе механизма преступления представляет собой актуальную задачу для отечественной криминалистики, поскольку она вызвана с одной стороны, насущными потребностями практики, а с другой – отсутствием таких систем в России в настоящее время. Между тем, можно прогнозировать, что при их создании будут возникать множественные проблемы. Рассмотрим некоторые из них.

#### *Полнота данных*

Очевидно, что эффективность, того или иного учёта определяется, в первую очередь, его содержанием, т. е. тем, сколько данных о преступлениях будет в нём содержаться. Однако в работах, посвящённых расследованию серийных преступлений, нередко отмечается, что одной из ключевых проблем, которые препятствуют оперативному раскрытию и расследованию таких деяний, является их совершение в условиях неочевидности<sup>9</sup>, т. е. в условиях дефицита или даже отсутствия информации о событии преступления и преступнике<sup>10</sup>. Исходя из этого, мы можем ожидать, что некоторые сведения, подлежащие внесению в учёт, будут систематически отсутствовать. Исследование данных, введённых в базу ViCLAS, проведённое французскими криминалистами, показало, что, как правило, в них отсутствовала информация о преступнике и его действиях<sup>11</sup>. При этом именно эти сведения сотрудники правоохранительных органов считают наиболее ценной, о чём свидетельствуют результаты проведённого нами анкетирования, согласно которым 137 человек (51,7 %) оценивали информацию о личности преступника как максимально полезную, а 152 человека (52,4 %) таким образом оценили информацию о его поведении.

#### *Ввод данных*

Прежде чем та или иная криминалистическая информация может быть использована в криминалистическом учёте, она должна быть перенесена из материалов уголовного дела в форму, пригодную для её хранения, обработки и передачи. В случае учёта по механизму преступлений этот процесс предполагает заполнение формы (анкеты, опросника и т. п.), содержащей в себе перечень вопросов, которые могут быть закрытыми (т. е. предполагать выбор из ограниченного перечня возможных вариантов ответов), открытыми (т. е.

---

<sup>8</sup> Созонов А. И. О практике расследования в системе Следственного комитета Российской Федерации серийных преступлений и преступлений прошлых лет // Раскрытие и расследование преступлений серийных и прошлых лет: материалы Международной научно-практической конференции (Москва, 16 марта 2017 года). М.: Московская академия Следственного комитета Российской Федерации, 2017. С. 25.

<sup>9</sup> См. например: Исаенко В. Н. Проблемы теории и практики расследования серийных убийств. М.: АНО «Юридические программы», 2005. С. 9.

<sup>10</sup> Белкин Р. С. Криминалистическая энциклопедия. М.: Изд-во «Мегатрон XXI», 2000. С. 182.

<sup>11</sup> Julien C., Aebi M. F. The Tree That Hides the Forest? Testing the Construct Validity of ViCLAS through an Empirical Study of Missing Data // Policing: A Journal of Policy and Practice. 2019. Vol. 13. № 1. P. 53.

предполагать, что лицо, заполняющее форму, самостоятельно вводит / пишет ответ) или же комбинированными (т. е. сочетающие оба предыдущих варианта).

Из этого вытекает целый спектр проблем.

Во-первых, это достижение единообразия при описании схожих элементов механизма преступления. Не вызывает сомнений, что для достаточно эффективного использования информации об элементах механизма преступления при сравнительном анализе, она должна быть описана схожим образом, в противном случае эти сведения могут быть даже полностью несопоставимы, что повлечёт за собой утрату пласта потенциально полезной информации.

Теоретически, эта проблема не должна возникать в том случае, когда используется закрытый список заранее сформулированных ответов, однако на практике, в силу гигантской вариативности содержания некоторых элементов механизма преступления, которые встречаются при расследовании реальных дел, ограничиться исключительно закрытым списком ответов, как минимум, нерационально, а часто – и вовсе невозможно.

Во-вторых, сложность представляет отражение криминалистической информации в сознании лица, которое переносит данные из материалов дела в учёт.

А. А. Давлетов справедливо отметил, что процесс отражения любого преступления можно разделить на два этапа: объективный (первичный), т. е. характеризующий возникновение реальной, объективно существующей материальной связи между событием преступления и окружающими его явлениями и вещами, и субъективный (вторичный), т. е. отражение события преступления в мышлении субъекта уголовно-процессуального познания на основе результатов предыдущего (объективного) этапа<sup>12</sup>.

Развивая эту мысль применительно к проблематике настоящего исследования, мы можем заключить, что, поскольку ввод данных в учёт осуществляется, как правило, на основе материалов уголовных дел, в которых зафиксированы результаты субъективного отражения, здесь возникает уже третичный этап отражения.

Проблема заключается в том, что каждый последующий этап отражения всегда влечёт за собой утрату части ранее отражённой информации. Подобно тому, так следователь или эксперт, участвующие в осмотре места происшествия, могут не отразить тот или иной след (соответственно, не зафиксировав его в протоколе, не изъяв и т. д.), так и лицо, осуществляющее ввод данных в учёт, может не заметить какую-либо деталь или неправильно её оценить.

#### *Количество данных*

На первый взгляд, может показаться очевидным, что чем больше сведений о механизме преступления будет внесено в учёт, тем больше пользы он сможет принести. Между тем, против этого можно выдвинуть ряд возражений.

---

<sup>12</sup> Давлетов А. А. Основы уголовно-процессуального познания. Екатеринбург: Издательство Гуманитарного университета, 1997. С. 26.

Во-первых, увеличение количества данных, подлежащих вводу в учёт, автоматически повлечёт за собой увеличение доли ошибочных сведений.

Во-вторых, слишком большое количество информации может повлечь за собой то, что за отдельными деталями преступлений, содержащимися в учёте, лицо может упустить общую картину преступлений. В результате возникает риск принятия как ложно-положительного (о том, что серия есть, когда на самом деле её нет), так и ложно-отрицательного (о том, что серия отсутствует, когда на самом деле она есть) решения о соединении или об отказе в соединении преступлений в серию.

Во-третьих, обильное количество информации, подлежащей анализу, может привести к информационной перегрузке, т. е. состоянию, в котором лицо сталкивается с настолько большой информационной нагрузкой, что утрачивает возможность принять оптимальное решение<sup>13</sup>.

#### *Алгоритмы обработки данных.*

За период времени с января по апрель 2024 года на территории РФ было совершено 630,8 тыс. преступлений, 31,5 % из которых относятся к категориям тяжких и особо тяжких<sup>14</sup>. Совокупность информации о таком количестве преступлений нельзя охарактеризовать иначе как «большие данные». Несмотря на повсеместную популярность этого термина, единообразное определение его отсутствует, тем не менее, принято считать, что большие данные характеризуются тремя особенностями: 1) гигантский объём; 2) высокая скорость накопления; 3) разнообразие, т. е. получение их из различных источников<sup>15</sup>. В связи с этим, обработка их традиционными средствами является либо невозможной, либо недопустимо продолжительной.

В связи с этим, криминалистический учёт, содержащий информацию о механизмах преступлений, должен включать в себя такие алгоритмы работы с данными, которые позволят автоматизировать большую часть процесса поиска и сравнительного анализа информации о механизмах преступлений, например, самостоятельно отсеивая очевидно несерийные преступления (используя, в частности, сведения о времени и местах их совершения), сводя конечный результат к такому объёму, который человек может самостоятельно обработать и делать этот достаточно быстро.

### **Список литературы**

1 Белкин Р. С. Криминалистическая энциклопедия. М.: Изд-во «Мегатрон XXI», 2000. 334 с.

---

<sup>13</sup> Roetzel P. G. Information overload in the information age: a review of the literature from business administration, business psychology, and related disciplines with a bibliometric approach and framework development // Business Research. 2019. № 12. P. 484.

<sup>14</sup> Состояние преступности в России за январь - апрель 2024 года. М.: ВНИИ МВД России, 2024. С. 2.

<sup>15</sup> Чехарин Е. Е. Большие данные: большие проблемы // Перспективы науки и образования. 2016. № 3. С. 7.

- 2 Бессонов А. А., Гайворонская А. А. Прайминг и его эффекты в получении криминалистически значимой информации // Вестник Томского государственного университета. 2021. № 466. С. 207–212.
- 3 Давлетов А. А. Основы уголовно-процессуального познания. Екатеринбург: Издательство Гуманитарного университета, 1997. 191 с.
- 4 Исаева Л. М. Психолого-криминалистическое портретирование: моногр. М.: ФГКУ ВНИИ МВД России, 2015. 143 с.
- 5 Исаенко В. Н. Проблемы теории и практики расследования серийных убийств. М.: АНО «Юридические программы», 2005. 304 с.
- 6 Сазонов А. И. О практике расследования в системе Следственного комитета Российской Федерации серийных преступлений и преступлений прошлых лет // Раскрытие и расследование преступлений серийных и прошлых лет: материалы Международной научно-практической конференции (Москва, 16 марта 2017 года). М.: Московская академия Следственного комитета Российской Федерации, 2017. С. 24–28.
- 7 Усманов Р. А. Теория и практика использования криминалистической информации в процессе раскрытия и расследования преступлений: монография. Челябинск: Челябинский юридический ин-т МВД России, 2006. 231 с.
- 8 Чехарин Е. Е. Большие данные: большие проблемы // Перспективы науки и образования. 2016. № 3. С. 7–11.
- 9 Collins P. I., Johnson G. F., Choy A., Davidson K. T., Mackay R. E. Advances in violent crime analysis and law enforcement: The canadian violent crime linkage analysis system // Journal of Government Information. 1998. Vol. 25. № 3. P. 277–284.
- 10 Fosdick R. B. The Modus Operandi System in the Detection of Criminals // Journal of the American Institute of Criminal Law and Criminology. 1915. Vol. 6. № 4. P. 560–570.
- 11 Julien C., Aebi M. F. The Tree That Hides the Forest? Testing the Construct Validity of ViCLAS through an Empirical Study of Missing Data // Policing: A Journal of Policy and Practice. 2019. Vol. 13. № 1. P. 55–56.
- 12 Roetzel P. G. Information overload in the information age: a review of the literature from business administration, business psychology, and related disciplines with a bibliometric approach and framework development // Business Research. 2019. № 12. P. 479–552.
- 13 Woodhams J., Davies K., Galambos S., Webb M. A Descriptive Analysis of the Temporal and Geographical Proximities Seen Within UK Series of Sex Offenses // Journal of Police and Criminal Psychology. 2021. Vol. 36. P. 706–715.

**Илья В. Леднев**

Postgraduate student of the Department of Criminalistics  
Ural State Law University named after V. F. Yakovlev  
(Yekaterinburg, Russian Federation)  
ilialednev@mail.ru

## PROBLEMS OF ACCOUNTING FOR THE MECHANISM OF THE OFFENCE

**Abstract:** The key to successful detection of any serial crimes is timely detection of their serial nature by law enforcement officers. An important role in this is played by various criminalistic records, especially the record on the mechanism of the committed crime, as the most universal. Unfortunately, at present, Russia lacks such records. Within the limits of the present article the author considers a number of problems which necessarily demand the decision during development and introduction in operation of such account.

**Keywords:** serial offences, crime mechanism, forensic accounting, forensic registration.

**Перевозникова Екатерина Юрьевна**

Соискатель,

Санкт-Петербургский государственный университет

(г. Санкт-Петербург, Российская Федерация)

[Ekaterinaperevoznikova@rambler.ru](mailto:Ekaterinaperevoznikova@rambler.ru)

## **СОВРЕМЕННОЕ СОСТОЯНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

**Аннотация:** В статье рассматривается текущее состояние преступности, связанной с использованием информационно-телекоммуникационных сетей. Отмечается, что развитие компьютерных технологий и доступность технических устройств способствуют росту количества преступлений в этой сфере. Проведён анализ статистических данных о преступлениях в России и некоторых зарубежных странах, который показал значительный рост киберпреступлений, тяжких и особо тяжких, с использованием сети Интернет и мобильной связи. Также рассматриваются специфические виды мошенничества и указывается на необходимость обновления защитных механизмов. В статье подчёркивается важность законодательных мер, образовательных кампаний, технологических решений и международного сотрудничества для борьбы с киберпреступностью.

**Ключевые слова:** киберпреступность, информационно-телекоммуникационные сети, интернет, мошенничество, законодательство, кибербезопасность.

Уголовное законодательство Российской Федерации на сегодняшний день не отличается оперативностью изменений в отношении преступлений, связанных с совершением общественно опасных деяний посредством использования информационно-телекоммуникационных сетей.

Проведённый анализ статистических данных по преступлениям, совершённым с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, показал, что на сегодняшний день преступления в сфере компьютерной информации составляют значительную часть в общей структуре преступности, а их количество стабильно увеличивается каждый год. Так, согласно статистическим данным, Министерством внутренних дел Российской Федерации в январе–декабре 2023 года зарегистрировано 677,0 тыс. преступлений, совершённых с использованием информационно телекоммуникационных технологий или в сфере компьютерной информации, что на 29,7 % больше, чем за аналогичный период прошлого года<sup>1</sup>. При этом, в общем числе зарегистрированных преступлений их удельный вес

---

<sup>1</sup> Состояние преступности в России за январь–декабрь 2023 года. Москва: МВД России, 2024. 64 с.

увеличился с 26,5 % в январе–декабре 2022 года до 34,8 %. Практически все такие преступления (98,8 %) выявляются органами внутренних дел. Больше половины таких преступлений (50,6 %) относится к категориям тяжких и особо тяжких (342,6 тыс.; + 25,9 %), более чем три четверти (77,8 %) совершается с использованием сети «Интернет» (526,8 тыс.; + 38,2 %), почти половина (44,7 %) – средств мобильной связи (302,9 тыс.; + 42,2 %).

Следует отметить, что из общего количества указанных преступлений в 2023 году зарегистрировано 342 637 тяжких и особо тяжких, что составляет 25,9 % от общего числа преступлений в данной сфере. Это указывает на значительный рост киберпреступности, а также позволяет сделать вывод об усиливающейся цифровой зависимости граждан и цифровизации различных аспектов жизнедеятельности.

Для зарубежных государств приведённая статистика так же актуальна. Анализ преступлений, совершённых с использованием сети Интернет в зарубежных странах, представляет особый интерес, поскольку позволяет сравнить и контрастировать подходы к кибербезопасности, законодательство и тенденции в различных регионах мира. Получение точных данных о преступлениях, совершённых с использованием сети Интернет в зарубежных странах, может быть затруднён из-за различий в методологиях сбора данных, но общий тренд с развитием технологий и расширением интернета положительный. Например, в отчёте Европейского центра по киберпреступности (ЕСЗ) указывается, что киберпреступность составляет значительную долю всех преступлений в Европе, и с каждым годом эта доля увеличивается. Согласно данным Международного союза телекоммуникаций (ITU), киберпреступность в 2020 году увеличилась на 600 % по сравнению с 2019 годом.

Кроме того, киберпреступные группировки постоянно разрабатывают новые методы и тактики, чтобы обойти существующие меры безопасности и получить доступ к чувствительной информации или совершить мошенничества в сети. В Соединённых Штатах Америки, по данным Федерального бюро расследований (FBI), киберпреступность также является значительной проблемой и её доля в общем объёме преступлений постоянно растёт. Статистика зарубежных стран показывает тенденции роста преступлений в следующих областях: кибермошенничество, кибербуллинг и онлайн-троллинг, детская порнография и сексуальные домогательства, кибертерроризм.

Возвращаясь к отчёту МВД России, укажем, что в нём также выделены специфические виды мошенничества, совершаемого с использованием фиктивных электронных платежей и компьютерной техники. Отдельно считаем необходимым выделить преступления, связанные с задействованием социальной инженерии, которая представляет собой целый комплекс методов, используемых злоумышленниками для получения конфиденциальной информации или доступа к закрытым системам путём манипуляций и обмана. Рассмотрим некоторые из основных современных схем социальной инженерии.

Одним из самых распространённых является фишинг (от англ. fishing – рыбачить, выуживать) – это вид кибератаки, при которой злоумышленник

пытается получить доступ к личной информации пользователя<sup>2</sup>. Злоумышленники рассылают электронные письма или сообщения, которые кажутся легитимными и призваны обманом заставить жертву раскрыть личную информацию, такую как пароли, номера кредитных карт и другие чувствительные данные. Часто такие письма содержат ссылки на поддельные сайты, имитирующие реальные.

Разновидностью фишинга, но с использованием телефонных звонков, является вишинг (голосовой фишинг – от англ. voice fishing). При данном виде преступления злоумышленники звонят жертве, представляясь сотрудниками банков, правоохранительных органов или других организаций, и под различными предлогами пытаются выведать личную информацию или убедить перевести деньги на подставной счёт.

Смишинг (SMS-фишинг) – похож на фишинг, но осуществляется через SMS-сообщения. Злоумышленники рассылают сообщения, содержащие ссылки на вредоносные сайты, или просят перезвонить по указанному номеру, чтобы получить конфиденциальную информацию.

В случае претекстинга (от англ. pretexting – предварительное представление) злоумышленник придумывает правдоподобный сценарий, чтобы получить от жертвы нужную информацию. Например, он может представиться сотрудником техподдержки и под предлогом решения несуществующей проблемы попросить логины и пароли от учётных записей.

Байтинг (от англ. bait – приманка) представляет собой метод, при котором злоумышленник оставляет заражённое устройство, например, USB-накопитель, в общественном месте, надеясь, что кто-то его найдёт и подключит к своему компьютеру. В результате жертва может установить вредоносное ПО, которое предоставляет доступ к системе злоумышленнику.

Разновидностью байтинга является байтинг через соцсети – использование поддельных аккаунтов в социальных сетях для завоевания доверия и получения информации от жертвы. При этом злоумышленники могут вступать в доверительные отношения, чтобы в дальнейшем воспользоваться этим для мошенничества.

Указанные разновидности преступлений, совершённые с использованием информационно-телекоммуникационных технологий (далее – ИКТ), подпадают под различные статьи Уголовного кодекса Российской Федерации (далее – УК РФ). Пленум Верховного Суда Российской Федерации в Постановлении № 37 от 26 сентября 2018 года «О судебной практике по делам о преступлениях, связанных с использованием информационно-коммуникационных технологий» (далее – Пленум ВС РФ № 37) уточняет применение этих статей.

Вместе с тем, сегодня существуют определённые проблемы при квалификации рассматриваемых преступлений, которые связаны как с техническими особенностями совершения преступлений, так и с юридическими

---

<sup>2</sup> Что такое фишинг и как защититься от фишинговых атак / Skillbox Media [Электронный ресурс]. URL: <https://skillbox.ru/media/code/chto-takoe-fishing-i-kak-ot-nego-zashchititsya/> (дата обращения: 20.05.2024).



асpekтами их квалификации, ведь в связи с быстрым развитием технологий законодательство не всегда успевает адаптироваться. В этой связи весьма значительным представляется организовывать сегодня работу по превенции подобных преступлений, так как предупредительные действия, по общему правилу, не требуют специальной нормативной регламентации.

Профилактика преступлений в гиперпреступной сети Интернет в зарубежных странах включает широкий спектр мер и действий, направленных на предотвращение, выявление и пресечение киберпреступности. Некоторые из ключевых методов профилактики включают в себя следующие направления:

1. Меры законодательного и правоохранительного характера, включающие развитие и усиление законодательства, касающегося киберпреступности, с целью ужесточения наказаний и обеспечения ответственности за киберпреступные действия.

2. Осуществление образовательной и просветительской деятельности с целью проведения образовательных кампаний для общественности, бизнеса и государственных организаций о рисках киберпреступности.

3. Разработка и внедрение технологических решений для защиты информации и сетевых систем от кибератак, включающих использование антивирусных программ, межсетевых экранов, систем обнаружения вторжений и шифрования данных.

4. Сотрудничество между правоохранительными органами различных стран для борьбы с киберпреступностью и обмена информацией о киберугрозах. Так, анализ сообщений потерпевших, как наиболее распространённого источника сведений о преступлениях в сфере компьютерной информации в таких странах как СНГ, Европейского союза, Соединенных Штатах, Австралии, Индии, Канаде<sup>3</sup>, улучшаются возможности выявления и расследования киберпреступлений на международном уровне. Также в указанных и некоторых других странах (в Великобритании – Action Fraud<sup>4</sup>, в Австралии – Центр кибербезопасности (ACSC)<sup>5</sup>) существуют специальные органы или подразделения, занимающиеся расследованием киберпреступлений.

5. Сотрудничество между государственными органами, частным сектором и академическими учреждениями для разработки и внедрения совместных инициатив по борьбе с киберпреступностью. Так, одним из примеров международной конвенции, направленной на укрепление сотрудничества между государствами в борьбе с киберпреступностью, является Конвенция Совета Европы о киберпреступности, также известная как Будапештская конвенция. Она была принята в 2001 году и в настоящее время

---

<sup>3</sup> См., например: Individuals & families // NCSC.GOV.UK [Электронный ресурс]. URL: <https://www.ncsc.gov.uk/section/information-for/individuals-families> (дата обращения: 20.08.2021); Phishing: Spot and report scam emails, texts, websites and... // NCSC.GOV.UK [Электронный ресурс]. URL: <https://www.ncsc.gov.uk/information/report-suspicious-emails> (дата обращения: 20.08.2021).

<sup>4</sup> Action Fraud. URL: <https://www.actionfraud.police.uk/> (дата обращения: 20.04.2024).

<sup>5</sup> Australian Cyber Collaboration Centre. URL: <https://www.cybercollaboration.org.au/> (дата обращения: 20.04.2024).

ратифицирована более чем 60 странами, включая большинство европейских государств, США, Канаду, Японию и другие.

В свою очередь, борьба с киберпреступностью в России в 2024 году включает в себя ряд мер и инициатив, направленных на предотвращение, выявление и пресечение киберугроз, среди которых можно выделить наиболее эффективные:

1. Усиление законодательства, внедрение новых и ужесточение существующих законов, касающихся киберпреступности, с целью увеличения санкций за совершение киберпреступлений и укрепления ответственности за нарушения в сети Интернет<sup>6</sup>. Так, впервые в уголовном законодательстве Российской Федерации Федеральным законом от 7 декабря 2011 года № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» в примечании к статье 272 Уголовного кодекса Российской Федерации<sup>7</sup> дано понятие компьютерной информации, как предмета преступления, к которому теперь относятся сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Также важное значение имеет принятое в 2022 году Постановление Пленума Верховного Суда Российской Федерации № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет»<sup>8</sup>, посвящённое в том числе применению уголовного закона по делам о преступлениях, предусмотренных гл. 28 УК РФ. К наиболее значимым разъяснениям Высшего судебного органа относятся: определение неправомерного доступа к компьютерной информации, преступных последствий по ст. 272 УК РФ, охраняемой законом информации, установления вины, допустимость квалификации содеянного как идеальной совокупности преступлений, предусмотренных ст. 272 и 273 УК РФ<sup>9</sup>.

---

<sup>6</sup> Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс». [Электронный ресурс]. URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_161817/](http://www.consultant.ru/document/cons_doc_LAW_161817/) (дата обращения: 20.05.2024).

<sup>7</sup> Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 06.04.2024) // СПС «КонсультантПлюс». [Электронный ресурс]. URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_10699/](http://www.consultant.ru/document/cons_doc_LAW_10699/) (дата обращения: 20.05.2024).

<sup>8</sup> Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет» // СПС «КонсультантПлюс». [Электронный ресурс]. URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_434573/](http://www.consultant.ru/document/cons_doc_LAW_434573/) (дата обращения: 17.05.2024).

<sup>9</sup> Щепельков В. Ф. О квалификации преступлений в сфере компьютерной информации (в свете разъяснений Пленума Верховного Суда РФ) // Уголовное право. 2023. № 6 (154). С. 70–79. DOI: 10.52390/20715870\_2023\_6\_70.

2. Развитие технических средств защиты и повышение уровня кибербезопасности путём разработки и внедрения современных технологий и программных средств для обнаружения, блокировки и предотвращения кибератак.

3. Сотрудничество и взаимодействие с различными организациями для обмена информацией о киберугрозах, совместной разработки мер по защите от киберпреступности и координации действий при обнаружении инцидентов.

4. Реализация образовательных кампаний для населения и бизнеса о рисках киберпреступности, методах защиты информации и безопасном поведении в интернете, а также подготовка и развитие квалифицированных специалистов в области кибербезопасности и киберпреступности через специализированные образовательные программы и курсы повышения квалификации.

5. Всестороннее взаимодействие с другими странами и международными организациями в обмене информацией о киберугрозах, совместном расследовании киберпреступлений и разработке мер по борьбе с киберугрозами на международном уровне.

Таким образом, можно заключить, что Российская Федерация предпринимает актуальные меры, направленные на предупреждение компьютерных преступлений, однако ими нельзя ограничиваться – необходимо и дальше совершенствовать законодательство в сфере разрешения негативных последствий подобных преступлений.

### **Список литературы**

1. Бурлаков В. Н. Плоткина Л. Н., Щурова А. С. Оптимизация прав человека на информацию в сети «Интернет» в контексте предупреждения распространения наркотиков // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 64–71.

2. Жижина М. В., Завьялова Д. В. Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников) // Актуальные проблемы российского права. 2022. № 5 (138). С. 149–158.

3. Фатьянов А. А., Григорьева М. А. Преступления в сфере компьютерной информации по законодательству Российской Федерации и штата Луизиана (США): сравнительно-правовой анализ // Российский следователь. 2022. № 8. С. 69–74. DOI: 10.18572/1812-3783-2022-8-69-74.

4. Щепельков В. Ф. О квалификации преступлений в сфере компьютерной информации (в свете разъяснений Пленума Верховного Суда РФ) // Уголовное право. 2023. № 6 (154). С. 70–79. DOI: 10.52390/20715870\_2023\_6\_70.

**Ekaterina Yu. Perevoznikova**  
Applicant,  
Saint Petersburg State University  
(Saint Petersburg, Russian Federation)  
Ekaterinaperevoznikova@rambler.ru

**THE CURRENT STATE OF LEGAL REGULATION OF CRIMES IN THE  
FIELD OF INFORMATION AND TELECOMMUNICATION  
TECHNOLOGIES**

**Abstract:** This article examines the current state of crime related to the use of information and telecommunication networks. It is noted that the development of computer technologies and the accessibility of technical devices contribute to the increase in the number of crimes in this area. An analysis of statistical data on crimes in Russia and some foreign countries shows a significant increase in cybercrime, including serious and especially serious offenses, involving the use of the Internet and mobile communications. The article also discusses specific types of fraud and the need to update security mechanisms. The importance of legislative measures, educational campaigns, technological solutions, and international cooperation in combating cybercrime is emphasized.

**Keywords:** cybercrime, information and telecommunication networks, Internet, fraud, legislation, cybersecurity.

**Рябчиков Сергей Александрович**  
Старший преподаватель кафедры криминалистики,  
Уфимский юридический институт МВД России  
(г. Уфа, Российская Федерация)  
r\_s.91@mail.ru

## **ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ КАК ЦЕНТРАЛЬНОЕ ЗВЕНО ЦИФРОВОЙ ПЛАТФОРМЫ УГОЛОВНОГО СУДОПРОИЗВОДСТВА**

**Аннотация:** Статья исследует роль электронного документооборота в контексте цифровизации правовой системы. Автор анализирует текущие методы производства по уголовным делам и отмечает, что введение электронных документов поспособствует модернизации этого процесса. Станет возможно документировать информацию в электронном виде, используя приёмы, способы и технологии сбора электронных доказательств. Автором рассматривается концепция создания единой цифровой платформы уголовного судопроизводства, которая должна содержать в себе модуль электронного уголовного дела и объединять уже имеющиеся цифровые платформы, реализующие функции отдельных участников уголовного судопроизводства в единую экосистему, где электронный документооборот является центральным звеном.

**Ключевые слова:** электронный документ, документооборот, электронное уголовное дело, цифровая платформа, уголовный процесс, электронные доказательства.

На современном этапе развития правовой системы России цифровизация приобретает всё большее значение. Внедрение информационных технологий в процесс производства по уголовным делам позволяет существенно увеличить его эффективность, снизить количество ошибок и повысить качество расследований. Один из ключевых аспектов этой трансформации – переход на электронный документооборот.

Электронный документооборот становится важным элементом современного уголовного судопроизводства и судебной системы России в целом. В эпоху цифровизации многие государства стремятся использовать новейшие технологии для повышения эффективности и прозрачности правосудия. В этом контексте судопроизводство, опирающееся на цифровые платформы и электронные документы, предоставляет целый ряд преимуществ, что делает электронный документооборот центральным звеном в таких системах.

Электронный документооборот представляет собой систему управления с использованием электронных документов. Эта система включает в себя создание, передачу, получение, хранение и обработку документов в цифровом

виде<sup>1</sup>. Правовой основой его использования являются: Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральный закон Российской Федерации от 25 марта 2011 г. № 63-ФЗ «Об электронной подписи» и иные нормативные правовые акты, регулирующие особенности его использования в государственных органах и учреждениях.

В уголовном судопроизводстве электронный документооборот может охватывать широкий спектр действий, таких как принятие электронного заявления о преступлении, создание постановления о возбуждении уголовного дела с автоматическим присвоением номера, направлением уведомления и копий решения участникам уголовного судопроизводства, создание электронных постановлений, протоколов и направление поручений о производстве следственных и иных процессуальных действий, а самое главное – своевременное взаимодействие органов уголовного преследования, участников уголовного процесса, стороны защиты и суда в электронной форме.

Текущее состояние уголовного судопроизводства не предусматривает систему электронного документооборота в полноценном виде. Части его проявления содержатся в отдельных статьях (ч. 3.1 ст. 222, ч. 2 ст. 393, ст. 474.1 и 474.2 УПК РФ). В основном все действия осуществляются с использованием бумажных документов. Однако это имеет ряд недостатков: возможность утраты документов как по случайным обстоятельствам (пожар, наводнение), так и в результате преднамеренных действий участников процесса (фальсификация, уничтожение); сложность поиска и анализа необходимой информации среди объёмных материалов уголовных дел; а также финансовые затраты на создание и использование материальных носителей.

Преимуществом производства по уголовным делам с использованием электронного документооборота является минимизация вышеуказанных недостатков, что позволит значительно сократить сроки уголовного судопроизводства, снизить нагрузку на органы предварительного расследования и суды, тем самым повысить научную организацию их труда.

Современное развитие цифровых технологий и повсеместное внедрение их результатов в общество поспособствовало перенесению многих функций жизнедеятельности человека в цифровую среду информационно-телекоммуникационной сети Интернет, результатом чего является появление больших объёмов электронной информации, а в контексте совершаемых преступлений – электронных следов, которые в настоящее время являются предметом обсуждения многих ученых<sup>2</sup>.

---

<sup>1</sup> Рябчиков С. А. Электронный документооборот в досудебном производстве по уголовным делам: современное состояние и развитие // Вестник Южно-Уральского государственного университета. Серия: Право. 2023. Т. 23. № 4. С. 29.

<sup>2</sup> См. напр.: Зуев С. В. Электронные доказательства в уголовном судопроизводстве: понятие и значение // Правопорядок: история, теория, практика. 2020. № 3 (26). С. 46–51; Никурадзе Н. О. «Электронные доказательства» в уголовном процессе: о целесообразности правового регулирования // Журнал российского права. 2024. № 4. С. 132–144; Пастухов П. С.

Совершенствуются способы совершения преступления. Например, при сбыте наркотических средств вознаграждение «наркосбытчик» получает криптовалютой. Фотографии закладок наркотических средств направляются и хранятся в облачных хранилищах, а не памяти устройства, на которое сделана фотография, что затрудняет процесс доказывания<sup>3</sup>.

Текущие методы классического уголовного процесса не готовы к реализации полноценного электронного доказывания с применением электронных доказательств, электронных документов и их оборота, «существующий порядок и правила производства большинства следственных действий разработаны для «бумажного» делопроизводства» и, как отметил профессор А. М. Баранов, «мало пригодны при переходе на электронный формат»<sup>4</sup>.

Применение электронного документооборота способствует сбору информации, имеющей значение для уголовного дела, в электронной форме, формированию электронных доказательств. Современные способы собирания электронной информации, такие как цифровая криминалистика (Digital Forensic), технологии анализа больших данных (Big Data), поиск информации, имеющей значения для уголовного дела, по открытым источникам (OSINT), и др., позволяют органам предварительного расследования собирать и использовать доказательственную информацию в электронном виде. К таким доказательствам относятся: «электронные сообщения, электронные документы и иные документы в электронной форме, цифровые аудио- и видеозапись, фотоизображение, информация интернет-порталов публичных органов и организаций, информация в СМИ, SMS-сообщения, бизнес-мессенджеры и социальные сети, электронные копии (образ) документа, цифровой отпечаток сайта (веб-архивы) и др.»<sup>5</sup>.

Отсутствие процессуальной регламентации использования вышеуказанных способов не позволяет органам расследования полноценно реализовать имеющиеся возможности сбора электронной доказательственной информации и использовать её в качестве электронных доказательств, которые отвечали бы требованиям относимости, допустимости и достоверности. В связи этим нами предлагается разработка и закрепление в УПК РФ универсальной нормы, позволяющей использовать приёмы, способы и технологии при работе с

---

Электронное вещественное доказательство в уголовном судопроизводстве // Вестник Томского государственного университета. 2015. № 396. С. 149–153.

<sup>3</sup> Апелляционное определение Воронежского областного суда от 18.10.2021 № 22-2463/2021. // СПС «КонсультантПлюс» [Электронный ресурс]. URL: <https://www.consultant.ru/> (дата обращения: 21.04.2024).

<sup>4</sup> Баранов А. М. Правила производства следственных действий или способов собирания доказательств // 25 лет на службе Отечеству: Сборник научных трудов, посвященный деятельности научных школ Санкт-Петербургского университета МВД России и приуроченной к 25-летию со дня его образования / Сост.: О. И. Городовая, О. С. Кравченко, А. А. Жаворонкова. Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2023. С. 329.

<sup>5</sup> Смирнов А. В. Электронные доказательства, электронное доказывание, искусственный интеллект: что далее? // Уголовное судопроизводство. 2024. № 1. С. 24–31.

электронными устройствами и информацией на них при производстве следственных действий.

Процесс расследования уголовных дел предусматривает не только сбор информации, имеющей доказательственное значение, но и взаимодействие участников уголовного судопроизводства. Как отмечалось выше, элементы электронного документооборота проявляются в уголовном судопроизводстве и осуществляются через отдельные цифровые платформы участников уголовного процесса.

Статья 474.1 УПК РФ предусматривает использование электронных документов в ходе судебного производства, что реализуется с использованием цифровой платформы Государственной автоматизированной системы «Правосудие» (ГАС «Правосудие»).

Статья 474.2 УПК РФ предусматривает порядок использования электронных документов в ходе досудебного производства, что, в частности, реализуется в органах предварительного расследования системы МВД России через цифровую платформу Единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России.

Сторона защиты взаимодействует со стороной обвинения и судом посредством Комплексной информационной системой адвокатуры России (КИС АР).

Иные лица, вовлекаемые в уголовное судопроизводство, имеют возможность взаимодействия через Федеральную государственную информационную систему «Единый портал государственных и муниципальных услуг (функций)» (далее ЕПГУ), являющейся цифровой платформой. Однако такое взаимодействие ограничено лишь некоторыми функциями: направлением заявлений и ходатайств в суды посредством ГАС «Правосудие» или в орган расследования посредством ИСОД МВД России.

Анализ показывает, что на данный момент функционируют различные цифровые платформы. Однако их интеграция в единую экосистему уголовного судопроизводства является существенной проблемой. Как справедливо отметил П. С. Пастухов, эта сложность заключается в организации и взаимодействии различных систем электронного документооборота<sup>6</sup>. Тем не менее, подобные вопросы могут быть решены на технологическом уровне посредством применения межведомственного электронного взаимодействия. По мнению А. Б. Смушкина, «трансформация цифровых технологий расследования в процессе внедрения их в форме цифровых платформ должна развиваться в полномасштабные экосистемы уголовного судопроизводства, синергетический эффект применения которых значительно повысит эффективность расследований»<sup>7</sup>.

---

<sup>6</sup> Пастухов П. С. Цифровые платформы как основа электронного документооборота в уголовном судопроизводстве // Пермский юридический альманах. 2023. № 6. С. 524.

<sup>7</sup> Смушкин А. Б. Об экосистеме предварительного расследования // Вестник Томского государственного университета. 2023. № 488. С. 245.



Таким образом, современная цифровая платформа уголовного судопроизводства это «оборудование, инфраструктура и программное обеспечение, обеспечивающее сетевое взаимодействие всех участников уголовного судопроизводства для внедрения электронных доказательств и использования электронного документооборота»<sup>8</sup>, где ключевыми в обеспечении современного уголовного процесса являются интернет-технологии, а центральным звеном – электронный документооборот, так как он обеспечивает интеграцию данных и координацию всех участников уголовного процесса. В будущем у участников появится возможность доступа к процессуальным документам в режиме реального времени, что значительно упростит возможность ознакомления с документами и ускорит процесс принятия решений.

В заключение отметим, что внедрение электронного документооборота в уголовное судопроизводство является важным шагом на пути цифровой трансформации правосудия России. Переход на него повысит эффективность и прозрачность уголовного процесса, сократит издержки, минимизирует риски утраты процессуальных документов, фальсификации, а также позволит собирать электронную информацию в виде электронных доказательств с формированием электронного уголовного дела. Создание единой цифровой платформы уголовного судопроизводства оптимизирует процессуальные действия и упростит взаимодействие между участниками процесса. Внедрение электронного документооборота как центрального звена станет важным инструментом модернизации правосудия и поспособствует созданию эффективной системы, отвечающей современным требованиям.

### **Список литературы**

1. Баранов А. М. Правила производства следственных действий или способов собирания доказательств // 25 лет на службе Отечеству: Сборник научных трудов, посвященный деятельности научных школ Санкт-Петербургского университета МВД России и приуроченной к 25-летию со дня его образования / Сост.: О. И. Городовая, О. С. Кравченко, А. А. Жаворонкова. Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2023. С. 325–330.

2. Высокотехнологичный уголовный процесс: монография / под ред. докт. юрид. наук С. В. Зуева, докт. юрид. наук Л. Н. Масленниковой. М.: Юрлитинформ, 2023. 216 с.

3. Зуев С. В. Электронные доказательства в уголовном судопроизводстве: понятие и значение // Правопорядок: история, теория, практика. 2020. № 3 (26). С. 46–51.

---

<sup>8</sup> Высокотехнологичный уголовный процесс: монография / под ред. докт. юрид. наук С. В. Зуева, докт. юрид. наук Л. Н. Масленниковой. М.: Юрлитинформ, 2023. С. 35.

4. Никурадзе Н. О. «Электронные доказательства» в уголовном процессе: о целесообразности правового регулирования // Журнал российского права. 2024. № 4. С. 132–144.
5. Пастухов П. С. Цифровые платформы как основа электронного документооборота в уголовном судопроизводстве // Пермский юридический альманах. 2023. № 6. С. 521–540.
6. Пастухов П. С. Электронное вещественное доказательство в уголовном судопроизводстве // Вестник Томского государственного университета. 2015. № 396. С. 149–153.
7. Рябчиков С. А. Электронный документооборот в досудебном производстве по уголовным делам: современное состояние и развитие // Вестник Южно-Уральского государственного университета. Серия: Право. 2023. Т. 23. № 4. С. 27–32.
8. Смирнов А. В. Электронные доказательства, электронное доказывание, искусственный интеллект: что далее? // Уголовное судопроизводство. 2024. № 1. С. 24–31.
9. Смушкин А. Б. Об экосистеме предварительного расследования // Вестник Томского государственного университета. 2023. № 488. С. 242–247.

**Sergey A. Ryabchikov**

Senior Lecturer at the Department of Criminology,  
Ufa Law Institute of the Ministry of Internal Affairs of Russia  
(Ufa, Russian Federation)  
r\_s.91@mail.ru

## **ELECTRONIC DOCUMENT MANAGEMENT AS THE CENTRAL LINK OF THE DIGITAL PLATFORM OF CRIMINAL PROCEEDINGS**

**Abstract:** The article explores the role of electronic document management in the context of digitalization of the legal system. The author analyzes the current methods of criminal proceedings and notes that the introduction of electronic documents will contribute to the modernization of this process. It will be possible to document information in electronic form using techniques, methods and technologies for collecting electronic evidence. The author considers the concept of creating a single digital platform for criminal proceedings, which should contain an electronic criminal case module and combine existing digital platforms that implement the functions of individual participants in criminal proceedings into a single ecosystem, where electronic document management is the central link.

**Keywords:** electronic document, document management, electronic criminal case, digital platform, criminal procedure, electronic evidence.

**Семенкова Евгения Викторовна**

Кандидат юридических наук, доцент кафедры уголовного процесса  
Московский университет МВД России имени В. Я. Кикотя  
(г. Москва, Российская Федерация)  
sevg22@yandex.ru

**ЭЛЕКТРОННОЕ УГОЛОВНОЕ ДЕЛО: ПОНЯТИЕ И ПЕРСПЕКТИВЫ  
ВНЕДРЕНИЯ В УГОЛОВНЫЙ ПРОЦЕСС РОССИИ**

**Аннотация:** Развитие современного общества приводит к необходимости внедрения в уголовный процесс России электронного производства на всех стадиях, что толкает практиков и учёных-процессуалистов не только к бурным дискуссиям о таких перспективах, но и к разработке возможных механизмов такой трансформации. В настоящей статье автором на основе анализа существующих научных изысканий дано определение уголовного дела, электронного уголовного дела, а также проанализированы возможные позитивные и негативные перспективы электронной формы расследования преступлений.

**Ключевые слова:** уголовный процесс, уголовно-процессуальная деятельность, уголовное дело, электронное уголовное дело, цифровое производство, уголовно-процессуальные документы, процессуальные действия, следственные действия.

В условиях всеобщей цифровизации процессуалисты всё чаще стали поднимать вопрос о внедрении в уголовный процесс специальной цифровой формы представления результатов уголовного судопроизводства, которую всё чаще называют электронным уголовным делом. Однако, говорить об определении данного термина в отрыве от понятия существующей ныне формы представления результатов процесса (уголовное дело) довольно сложно. В этой связи полагаем необходимым определиться с понятием «уголовное дело». Тем более, что оно, на наш взгляд, имеет более широкий смысл, в то время как электронное уголовное дело является лишь одной из форм представления результатов уголовного судопроизводства, то есть одной из форм уголовного дела.

Уголовно-процессуальный кодекс не содержит легального определения дефиниции «уголовное дело», однако законодатель не отказывается от употребления данного термина, с которым можно столкнуться практически в каждой статье. Если точнее, то в уголовно-процессуальном кодексе термин «уголовное дело» в различных склонениях используется более девятисот раз.

В связи с отсутствием легального определения дефиниции «уголовное дело» в теории уголовного процесса существуют различные взгляды на данное понятие.

Многие учёные-процессуалисты предлагают рассматривать уголовное дело как многоаспектное явление. Например, О. В. Волынская полагает, что уголовное дело можно представить как юридическое производство, жизненный случай или как совокупность документов<sup>1</sup>. Сложно не согласиться с данной позицией, поскольку автор не выделяет специфические черты рассматриваемой дефиниции, используя довольно широкие категории, в которые вне сомнений можно включить и уголовное дело. Так, юридическое производство по своей сути – это все виды производств, существующих в России и закрепленных в основном законе страны. Одним из них является уголовное. Жизненный случай и вовсе предполагает любое событие, даже выходящее за область юридического поля, но не исключающее рассматриваемое понятие. Совокупность документов также представляется весьма расплывчатым термином, поскольку определённый комплект документов может быть сформирован по поводу различных фактов и в различных областях, например, такой же совокупностью можно назвать и медицинскую карту, однако и исключать из данного перечня уголовное дело тоже неверно.

И. Н. Гимазетдинова также предлагает рассматривать уголовное дело в различных, однако, уже более определённых аспектах: 1) как вид государственной деятельности; 2) как структурированную совокупность материалов по результатам всех проведённых процессуальных действий, в том числе поступающих ходатайств, жалоб и иных приобщённых материалов, имеющих отношение к противоправному деянию<sup>2</sup>.

Позволим себе не согласиться с позицией И. Н. Гимазетдиновой об уголовном деле как о виде государственной деятельности по следующим основаниям. Во-первых, полагаем, что считать уголовное дело каким-либо видом деятельности не совсем верно, поскольку сам термин не может подразумевать деятельность, но лишь отражение (фиксацию) результатов такой деятельности, в связи с чем в УПК РФ можно встретить словосочетания «возбуждение уголовного дела», «прекращение уголовного дела», «участие в уголовном деле», «производство по уголовному делу», то есть данный термин всегда употребляется с глаголом, обозначающим определённое действие с делом. Уголовное дело – это всегда какие-то материалы, составляемые по итогам осуществления определённых процессуальных действий, но не сама деятельность. По второй части определения уголовного дела, данного автором, нельзя не согласиться в части структурированности совокупности материалов, однако, на наш взгляд, неточность возникает из-за того, что автор не сделал акцента на уголовном судопроизводстве, осуществляемом по поводу деяния, предусмотренного именно уголовным законом, а не просто противоправного.

---

<sup>1</sup> Волынская О. В. Некоторые подходы к формулированию понятия «прекращение уголовного дела» // Российский следователь. 2006. № 3. С. 13–16.

<sup>2</sup> Гимазетдинова И. Н. Уголовное дело как комплексный процессуальный акт и возможность его перевода в электронный формат // Вестник Волгоградской академии МВД России. 2023. № 2 (65). С. 70–75.

Кроме того, определение автора не совсем ясно отражает форму осуществляемого производства (материальная или электронная).

Небезынтересной, но достаточно спорной представляется позиция В. В. Кониной, который также рассматривает уголовное дело с одной стороны как многоаспектную систему, объединяющую в себе оперативно-розыскные, следственные, процессуальные и судебные решения, а с другой стороны – как систематизированные документы, содержащие информацию о проведенных в процессе расследования оперативно-розыскных, судебных, следственных, процессуальных действиях<sup>3</sup>. На наш взгляд, включение в определение уголовного дела документов, которые отражают решения о проведении и результаты проведения оперативно-розыскных мероприятий не допустимо, поскольку накопление таких материалов предусмотрено в рамках дел оперативного учёта, а не уголовных; УПК РФ допускает использование в доказывании таких материалов лишь если они не противоречат закону (ст. 89 УПК РФ), при этом такого вида доказательств как результаты оперативно-розыскной деятельности не существует (ст. 74 УПК РФ). Выделение автором в определении следственных и процессуальных решений также представляется не совсем верным ввиду того, что все решения по уголовному делу являются процессуальными, как решения следователя, так и дознавателя и суда.

Довольно простой и понятной для восприятия является позиция И. И. Шереметьева, который предлагает считать уголовным делом физическую его основу, то есть систематизированные определённым образом уголовно-процессуальные, а также иные, технические, документы, типа описей, писем и т. д., но именно письменных, изложенных на бумажных носителях<sup>4</sup>. Полагаем, что такая позиция наиболее приемлема, тем более что в настоящее время иной формы уголовного дела, кроме материальной, уголовно-процессуальным законом не предусмотрено. Вместе с тем, такое определение не отражает принадлежности документов к определённым стадиям уголовного процесса, так как уголовно-процессуальные документы имеют место и в стадии исполнения приговора, например, при рассмотрении вопроса об условно-досрочном освобождении, однако материалами уголовного дела они не являются, хотя являются частью уголовного судопроизводства.

Основываясь на вышеизложенном, полагаем, что *уголовное дело – это определённая законом форма представления результатов предварительного расследования, а также разрешения уголовного спора в суде, служащая для накопления и систематизации документов, отражающих ход и результаты уголовно-процессуальной деятельности, и включающая в себя оформленные в установленном законом порядке протоколы следственных, судебных, иных процессуальных действий и решений, а также иные материалы, имеющие значение для установления обстоятельств, подлежащих доказыванию, и*

---

<sup>3</sup> Конин В. В. Термин «уголовное дело»: что под этим следует понимать? // Современное право. 2021. № 8. С. 115.

<sup>4</sup> Шереметьев И. И. Электронное уголовное дело: что это такое и пути его создания // Lex Russica (Русский закон). 2020. Т. 73. № 10 (167). С. 83.

*принятия итогового решения в суде в связи с совершением конкретного деяния, ответственность за которое предусмотрена УК РФ.* В данном определении намеренно не указано на материальную форму выражения результатов расследования, так как, на наш взгляд, используемая формулировка «определённая законом» даёт возможности для использования данного определения в том числе и в случае узаконивания электронного формата ведения уголовного производства. То есть данное определение как раз может относиться как к ныне существующему формату уголовного дела, так и к будущему формату электронного уголовного дела.

В то же время в теории уголовного процесса существуют различные определения электронного уголовного дела. Так, по мнению В. В. Кони́на, А. В. Кудрявцевой, А. В. Петрова электронное или, как его называют авторы, цифровое уголовное дело может представлять собой материалы оперативно-розыскных, следственных и судебных действий, которые собраны в одной базе, выполнены или сохранены в цифровом виде на электронном носителе и относятся к расследуемому преступлению<sup>5</sup>. По нашему мнению, такое определение не лишено недостатков, часть из которых ранее уже была проанализирована (включение материалов оперативно-розыскной деятельности в состав уголовного дела). Нужно отметить, что такое определение электронного уголовного дела говорит лишь об оцифровывании материалов, собранных по результатам расследования, но не отражает возможности производства процессуальных действий, в том числе принятие решений, с использованием специально разработанной программы.

С этой точки зрения заслуживающими внимания представляются позиции С. В. Зуева, Л. В. Бертовского, С. А. Степанова, которые предлагают под электронным уголовным делом понимать не просто специальные базы по накоплению материалов в оцифрованном виде, а специальные программы, которые позволят проводить следственные и процессуальные действия в онлайн-формате, в частности, технологию блокчейн<sup>6</sup>. Полностью поддерживаем данную позицию, полагая, что только специальная программа, позволяющая осуществить процессуальные действия в онлайн-формате, в том числе с удостоверением таких действий всеми участвующими лицами, действительно может позволить упростить процесс, но никак не банальное оцифровывание материалов на бумажных носителях, которое лишь усложнит процесс и увеличит

---

<sup>5</sup> Конин В. В., Кудрявцева А. В., Петров А. В. Уголовное дело- переход от бумажного носителя в цифровой формат // Вестник Томского государственного университета. Право. 2022. № 45. С. 94.

<sup>6</sup> Бертовский Л. В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. № 6. С. 226–230; Зуев С. В. Электронное уголовное дело: за и против // Правопорядок: история, теория, практика. 2018. № 4 (19). С. 6–12; Степанов С. А. Электронное уголовное дело: дань моде или современные тенденции развития уголовного судопроизводства // Уголовная политика в сфере обеспечения прав и законных интересов участников уголовного судопроизводства и использования современных технологий: Материалы Всероссийской (национальной) научно-практической конференции. Красноярск, 2021. С. 113–122.

и так существующую сегодня огромную нагрузку на органы предварительного расследования и суд.

Определившись с понятиями уголовного дела и электронного уголовного дела, вернёмся к вопросу о возможностях внедрения цифровых технологий в уголовный процесс России. Обсуждение этого вопроса довольно бурно ведётся в кругах учёных-процессуалистов, которые высказываются о наличии как отдельных плюсов, так и минусов<sup>7</sup>. При этом все приходят к общей мысли о неизбежности перевода производства по уголовным делам в электронный (цифровой) формат. Многие зарубежные страны сегодня уже стали новаторами во внедрении информационно-телекоммуникационных технологий в национальное законодательство, в том числе регулирующее производство по уголовным делам. К таковым относятся Сингапур, Швеция, Нидерланды, Дания, Бельгия, Канада, США, Саудовская Аравия, Грузия, Казахстан и ряд других, опыт которых должен быть учтён при цифровизации уголовного процесса России.

Вне сомнений к положительным свойствам цифровизации уголовного процесса можно отнести:

- 1) сокращение сроков производства по уголовным делам;
- 2) экономию ресурсов, как человеческих, так и материальных (сокращение расходов на бумагу, технику, места хранения уголовных дел и т. д.);
- 3) упрощение возможностей участников уголовного судопроизводства: к участию в производстве следственных действий; к взаимодействию с органами и должностными лицами, осуществляющими производство по уголовным делам; к материалам уголовного дела как на этапе окончания предварительного расследования, так и отражающим процессуальные действия с участием конкретного лица;
- 4) аналогичное упрощение осуществления процессуальных действий для должностных лиц, в том числе по направлению повесток (уведомлений), согласованию решений, ознакомлению с принятыми решениями заинтересованных лиц;
- 5) обеспечение прозрачности и доступности уголовного процесса для участвующих лиц.

Кроме того, отдельные авторы отмечают и другие положительные черты: сохранность результатов расследования от порчи, утери, уничтожения<sup>8</sup>; систематизация и структурирование материалов уголовного дела; возможность

---

<sup>7</sup> Качалова О. В., Цветков Ю. А. Электронное уголовное дело – инструмент модернизации уголовного судопроизводства // Российское правосудие. 2015. № 2 (106). С. 95-101; Зуев С. В. Электронное уголовное дело: за и против // Правопорядок: история, теория, практика. 2018. № 4 (19). С. 6–12; Гимазетдинова И. Н. Уголовное дело как комплексный процессуальный акт и возможность его перевода в электронный формат // Вестник Волгоградской академии МВД России. 2023. № 2 (65). С. 70-75.

<sup>8</sup> Гимазетдинова И. Н. Уголовное дело как комплексный процессуальный акт и возможность его перевода в электронный формат // Вестник Волгоградской академии МВД России. 2023. № 2 (65). С. 73.

автоматизированного ведения статистики по уголовным делам; снижение риска фальсификаций и исправлений<sup>9</sup> и т. д.

Однако, на наш взгляд, практически каждое положительное свойство имеет вторую сторону медали и может обернуться отрицательным. Именно поэтому, оценивая положительные качества электронного формата уголовных дел, многие процессуалисты также говорят о дальнесрочной перспективе по реализации внедрения цифровой формы представления результатов в уголовном процессе. По большей части это связано с отсутствием существующих ныне механизмов по формированию таких электронных уголовных дел. В этой связи полагаем, что для современного российского уголовного процесса определённые сложности внедрения цифровых технологий связаны со следующими фактами:

1) отсутствие нормативно-правового регулирования в части оформления результатов уголовно-процессуальной деятельности в цифровом формате;

2) необходимость разработки специального программного обеспечения и реализации сложных процессов его внедрения в уголовно-процессуальную деятельность;

3) необходимость обеспечения хранения большого объёма данных при должном обеспечении безопасности функционирования систем;

4) необходимость должного технического оснащения лиц, осуществляющих уголовное судопроизводство (ноутбуки, планшеты, стилусы, постоянный доступ к общегосударственной компьютерной сети, обеспечивающей передачу и сохранение данных);

5) необходимость обучения участников уголовного судопроизводства пользованию разработанной программой, как со стороны лиц, осуществляющих уголовное судопроизводство, так и иных.

Данные проблемы изложены весьма широко, каждая из них имеет свои негативные последствия, например, прорехи в нормативно-правовом регулировании влекут за собой незаконность осуществляемых действий и принимаемых решений, то есть, по сути, каждый этап работы в специальной программе должен быть подробно регламентирован, закон должен служить своеобразной инструкцией для работы с программой для участников процесса. Нарушения и сбои в обеспечении безопасности также приводят к определённым негативным последствиям, которые связаны как с возможными взломами систем и несанкционированными доступами, так и с полным уничтожением данных. Естественно, что все это в конечном итоге ведёт к нарушению прав и законных интересов участников уголовного судопроизводства.

Подводя итог, отметим, что человечество не стоит на месте, общество и государство постоянно развиваются и то, что ещё вчера казалось фантастикой, сегодня становится повседневными элементами нашей жизни. Поэтому цифровизация уголовного процесса и переход от бумажной материальной формы уголовных дел к электронной – это лишь вопрос времени и запроса общества. Думается, что современное состояние уголовного судопроизводства

---

<sup>9</sup> Качалова О. В., Цветков Ю. А. Электронное уголовное дело – инструмент модернизации уголовного судопроизводства // Российское правосудие. 2015. № 2 (106). С. 98.



пока не готово к полному переходу на цифровой формат по ряду факторов, которые изложены выше, однако постепенная цифровизация уже началась и имеется твёрдая уверенность, что в недалеком будущем производство по уголовным делам обернётся новым видом трансформации российского общества.

### **Список литературы**

1. Бертовский Л. В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. № 6. С. 226–230.
2. Волынская О. В. Некоторые подходы к формулированию понятия «прекращение уголовного дела» // Российский следователь. 2006. № 3. С. 13–16.
3. Гимазетдинова И. Н. Уголовное дело как комплексный процессуальный акт и возможность его перевода в электронный формат // Вестник Волгоградской академии МВД России. 2023. № 2 (65). С. 70–75.
4. Зуев С. В. Электронное уголовное дело: за и против // Правопорядок: история, теория, практика. 2018. № 4 (19). С. 6–12.
5. Качалова О. В., Цветков Ю. А. Электронное уголовное дело – инструмент модернизации уголовного судопроизводства // Российское правосудие. 2015. № 2 (106). С. 95–101.
6. Конин В. В. Термин «уголовное дело»: что под этим следует понимать? // Современное право. 2021. № 8. С. 114–118.
7. Конин В. В., Кудрявцева А. В., Петров А. В. Уголовное дело- переход от бумажного носителя в цифровой формат // Вестник Томского государственного университета. Право. 2022. № 45. С. 88–99.
8. Степанов С. А. Электронное уголовное дело: дань моде или современные тенденции развития уголовного судопроизводства // Уголовная политика в сфере обеспечения прав и законных интересов участников уголовного судопроизводства и использования современных технологий: Материалы Всероссийской (национальной) научно-практической конференции. Красноярск, 2021. С. 113–122.
9. Шереметьев И. И. Электронное уголовное дело: что это такое и пути его создания// Lex Russica (Русский закон). 2020. Т. 73. № 10 (167). С. 81–90.

**Evgeniya V. Semenkova**

Candidate of Law, Associate Professor of the Department of Criminal Procedure  
Moscow University of the Ministry of Internal Affairs of Russia  
named after V. Ya. Kikot  
(Moscow, Russian Federation)  
sevg22@yandex.ru

## **ELECTRONIC CRIMINAL CASE: THE CONCEPT AND PROSPECTS OF IMPLEMENTATION IN THE CRIMINAL PROCESS OF RUSSIA**

**Abstract:** The development of modern society leads to the need to introduce electronic production into the criminal process of Russia at all stages, which pushes practitioners and process scientists not only to heated discussions about such prospects, but also to develop possible mechanisms for such transformation. In this article, the author, based on the analysis of existing scientific research, defines a criminal case, an electronic criminal case, and analyzes possible positive and negative prospects for the electronic form of criminal investigation.

**Keywords:** criminal procedure, criminal procedural activity, criminal case, electronic criminal case, digital production, criminal procedural documents, procedural actions, investigative actions.

**Сергеев Алексей Михайлович**

Аспирант,

Департамент правового регулирования экономической деятельности,  
Финансовый университет при Правительстве Российской Федерации

(г. Москва, Российская Федерация)

alexei\_sergeev@mail.ru

## **ОБЗОР ИСТОЧНИКОВ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ АВТОНОМНЫХ ТРАНСПОРТНЫХ СРЕДСТВ**

**Аннотация:** Настоящая статья посвящена анализу системности правового регулирования использования автономных транспортных средств. Автор рассматривает перспективы развития источников такого регулирования. Подчёркивается отсутствие международного права в данной сфере, а принятие каких-либо международно-правовых соглашений или конвенций видится бесперспективным. Указывается на наличие в Конституции Российской Федерации необходимых основ для регулирования научно-технологического прогресса в сфере использования автономных транспортных средств. Предполагается, что недавний Указ Президента о национальных целях развития (№ 309) станет предвестником широкого законодательного и доктринального интереса. Федерального закона, регламентирующего использование автономных транспортных средств, в России до настоящего времени не принято. Автор рассматривает концептуальные проблемы ранее выдвинутых законодательных инициатив. С учетом недостатков предшествующих законопроектов предлагается общая идея закона с возможным наименованием «Об основах правового режима автономных транспортных средств».

**Ключевые слова:** беспилотные транспортные средства, инновационные транспортные средства, автономные транспортные средства, высокоавтоматизированные транспортные средства, правовые режимы, источники права.

Одним из перспективных направлений развития российской экономики является разработка и использование инновационных транспортных средств в различных сферах общественной жизни. Чёткого, системного, внутренне непротиворечивого правового регулирования использования технологически ёмких средств пока не выработано. Проблема состоит не в определении «профильной» отрасли права для беспилотных наземных транспортных средств, а в рационализации сочетания регулятивных потенциалов разных отраслей права. Более того, даже в формулировании понятийного аппарата наблюдаются неопределённости: подчёркивается, например, необходимость разграничения автономных транспортных средств и беспилотных транспортных средств, а

также выделения более широкого понятия – «инновационные транспортные средства»<sup>1</sup>.

Не обошёл стороной данную тему и Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года». Подпункт «а» пункта 7 данного Указа устанавливает ключевые показатели национальной цели «Технологическое лидерство»<sup>2</sup>, направленной на обеспечение технологической независимости и формирование новых рынков по ряду направлений, включая автономные транспортные средства, обеспечивающие транспортную мобильность населения.

Без сомнения, Указ Президента России о национальных целях развития станет ключевым ориентиром, так как закладывает важные цели, запускает дискуссии о том, как и за счёт чего будут реализовываться поставленные задачи. Предполагаем, что терминология, использованная в этом акте, в дальнейшем будет подхвачена и раскрыта не только различными государственными органами, представителями власти, но и учёными-цивиристами. Также и для целей настоящей статьи представляется необходимым использовать предложенный в Указе термин – автономные транспортные средства.

Конкретизируя сказанное, отметим, что насущная задача современности состоит в формировании правового режима эксплуатации автономных транспортных средств. Удачным представляется определение правового режима, предложенное Г. С. Беляевой. Учёный понимает под ним особый порядок правового регулирования общественных отношений, основанный на определённом сочетании правовых средств и способов правового регулирования (дозволений, запретов и позитивных обязанностей), направленный на достижение соответствующих правовых целей и планируемого оптимального социально-значимого результата<sup>3</sup>. Не вызывает сомнений, что использование автономных транспортных средств требует оформления *особого* правового режима, отличающегося от регламентации традиционных транспортных средств ввиду особых технических особенностей. Это направлено на достижение социально-значимого результата – создания условий для безопасного использования автономных транспортных средств.

Для формирования правового режима использования автономных транспортных средств необходимо наличие системы правовых регуляторов – источников права.

В первую очередь необходимо остановиться на международной регламентации, где какого-либо единого нормативно-правового акта (нормативного договора – конвенции, соглашения и т. п.) не выработано.

---

<sup>1</sup> См. Вавилин Е. В. Беспилотные транспортные средства: от терминологии к новым правовым режимам // Хозяйство и право. 2023. № 8. С. 3–21.

<sup>2</sup> Указ Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Официальный интернет-портал правовой информации pravo.gov [Электронный ресурс]. URL: <http://publication.pravo.gov.ru/document/0001202405070015> (дата обращения 20.05.2024).

<sup>3</sup> См. Беляева Г. С. Правовой режим: понятие и признаки // Вестник РУДН. Серия: Юридические науки. 2021 Т. 25. № 1. С. 281–293.

Учёными проводятся исследования зарубежного опыта правового регулирования использования беспилотных транспортных средств, однако они скорее показывают, что в каждом государстве выбирается свой, оригинальный путь оформления правового режима данных наземных средств<sup>4</sup>. При этом предполагаем, что принятие единого международного соглашения об использовании автономных транспортных средств на сегодняшний день нереалистично.

Даже на региональном международном уровне нет заметных инициатив по нормативному оформлению режима автономных транспортных средств. В 2011 г. было принято решение Таможенного союза, утвердившее Технический регламент «О безопасности колесных транспортных средств»<sup>5</sup>. Пункт 16 документа прямо указал, что требования безопасности использования *инновационных* транспортных средств устанавливаются решением уполномоченного органа по техническому регулированию государства – члена Таможенного союза, в котором проводится оценка соответствия.

Если переходить на национальный уровень, можно указать, что Конституция РФ<sup>6</sup> о правовом режиме автономных транспортных средств ожидаемо не упоминает – данный вопрос всё же является предельно точечным для регулирования на уровне основного закона государства. Однако в федеральном ведении находятся «федеральные транспорт и пути сообщения». Более того, в результате принятия Закона о поправке к Конституции 2020 г.<sup>7</sup> были закреплены конституционные основы научно-технологического прогресса. Теперь в Конституции указано, что соответствующая политика относится к предмету ведения Российской Федерации. Анализируя тренды, можно сделать вывод о том, что основные правовые рамки данного вопроса будут устанавливаться на федеральном уровне, в первую очередь Президентом и Правительством РФ.

Ранее нами рассматривался вопрос о том, что при определении субъектного состава правоотношений по использованию автономных транспортных средств актуальны положения, уже содержащиеся в гражданском законодательстве<sup>8</sup>. В продолжение тезиса отметим, что потенциал Гражданского

---

<sup>4</sup> См.: Дремлюга Р. Ю., Яковенко А. А. Регулирование тестирования беспилотного автотранспорта: опыт Европы // Азиатско-тихоокеанский регион: экономика, политика, право. 2020. № 1. С. 103–117.

<sup>5</sup> Решение Комиссии Таможенного союза от 09.12.2011 № 877 «О принятии технического регламента Таможенного союза “О безопасности колесных транспортных средств”» // СПС «КонсультантПлюс» [Электронный ресурс]. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_125114/](https://www.consultant.ru/document/cons_doc_LAW_125114/) (дата обращения 20.05.2024).

<sup>6</sup> Конституция Российской Федерации // Официальный интернет-портал правовой информации [pravo.gov.ru](http://pravo.gov.ru) [Электронный ресурс]. URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102027595> (дата обращения: 20.05.2024).

<sup>7</sup> Закон РФ о поправке к Конституции РФ от 14.03.2020 № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти» // Российская газета. 2020. № 55.

<sup>8</sup> См.: Сергеев А. М., Демченко М. В. Субъектный состав правоотношений, возникающих при использовании инновационных (беспилотных) транспортных средств в предпринимательской

кодекса Российской Федерации<sup>9</sup> более чем достаточен для установления основ частноправовых режимов использования автономных транспортных средств. Включение непосредственно в ГК РФ каких-либо новых структурных разделов видится излишним.

При этом дальнейшая активизация использования автономных транспортных средств определённо потребует развития публично-правового регулирования. В качестве примера можно привести Кодекс Российской Федерации об административных правонарушениях<sup>10</sup>, который какую-либо специальную административную ответственность применительно к эксплуатации автономных транспортных средств не закрепляет. Не предлагается соответствующих норм и в новых проектах законодательства об административных правонарушениях<sup>11</sup>.

В целом же публично-правовое регулирование использования автономных транспортных средств пока носит фрагментарный характер. Е. В. Гоц причину такого положения вещей видит в запоздалом внимании законодателя к данной сфере регулирования<sup>12</sup>. При этом учёный отмечает: построение системы подзаконных актов возможно только после решения вопросов принципиального и наиболее общего характера<sup>13</sup>.

Явным образом прослеживается необходимость принятия общего закона об использовании автономных транспортных средств, который должен стать своеобразным общим знаменателем между частноправовым и публично-правовым регулированием. В 2019 г. депутатом Государственной Думы РФ С. А. Жигаревым был подготовлен законопроект «Об опытной эксплуатации инновационных транспортных средств и внесении изменений в отдельные законодательные акты Российской Федерации», так и не ставший, однако,

---

деятельности // Проблемы экономики и юридической практики. 2024. Т. 20. № 1. С. 64–69. DOI: 10.33693/2541-8025-2024-20-1-64-69.

<sup>9</sup> Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ // Собрание законодательства РФ. 1996. № 5.

<sup>10</sup> Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Российская газета. 2001. № 256.

<sup>11</sup> См. напр. проект КоАП РФ, подготовленный Министерством юстиции РФ: проект федерального закона «Кодекс Российской Федерации об административных правонарушениях» // Федеральный портал проектов нормативных правовых актов. URL: <https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=102447> (дата обращения: 28.02.2024).

<sup>12</sup> См. Гоц Е. В. Вопросы публично-правового регулирования общественных отношений, связанных с внедрением инновационных транспортных средств в России: историко-правовой анализ // Транспортное право. 2023. № 4. С. 7–10.

<sup>13</sup> Гоц Е. В. Вопросы публично-правового регулирования общественных отношений, связанных с внедрением инновационных транспортных средств в России: историко-правовой анализ // Транспортное право. 2023. № 4. С. 7–10.

федеральным законом<sup>14</sup>. Причиной этому выступили как недостатки юридической техники, так и концептуальная незавершенность законопроекта<sup>15</sup>.

В 2020 г. законодательную инициативу проявил Государственный Совет Республики Татарстан, внёсший в Государственную Думу законопроект «Об инновационных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации»<sup>16</sup>. Эта инициатива была отклонена по формальным основаниям: отсутствие заключения Правительства РФ и увеличение расходов федерального бюджета.

В 2021 г. Министерством транспорта Российской Федерации был разработан альтернативный законопроект с наименованием «О высокоавтоматизированных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации»<sup>17</sup>. Этот проект нормативного правового акта преследовал несколько целей. В первую очередь разработчики законопроекта, очевидно, стремились конкретизировать понятийный аппарат в регулируемой сфере. В качестве собирательного термина предложили термин «высокоавтоматизированное транспортное средство». Эта попытка оказалась неудачной: в отрицательном заключении по итогам оценки регулирующего воздействия особо отмечалась неясность соотношения высокоавтоматизированного транспортного средства и инновационного транспортного средства.

Основное замечание Министерства экономического развития РФ, проводившего оценку регулирующего воздействия, сводится к избыточности юридических конструкций, а именно в возложении на физических и юридических лиц излишних обязанностей, запретов, ограничений, а также в провоцировании у пользователей высокоавтоматизированных транспортных средств чрезмерных финансовых затрат<sup>18</sup>.

---

<sup>14</sup> Законопроект № 710083-7 «Об опытной эксплуатации инновационных транспортных средств и внесении изменений в отдельные законодательные акты Российской Федерации» // Система обеспечения законодательной деятельности. URL: <https://sozd.duma.gov.ru/bill/710083-7> (дата обращения: 28.02.2024).

<sup>15</sup> См. критику отдельных аспектов законопроекта: Сергеев А. М., Демченко М. В. Субъектный состав правоотношений, возникающих при использовании инновационных (беспилотных) транспортных средств в предпринимательской деятельности // Проблемы экономики и юридической практики. 2024. Т. 20. № 1. С. 64–69. DOI: 10.33693/2541-8025-2024-20-1-64-69.

<sup>16</sup> Законопроект № 910152-7 «Об инновационных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации» // Система обеспечения законодательной деятельности. URL: <https://sozd.duma.gov.ru/bill/910152-7> (дата обращения: 29.02.2024).

<sup>17</sup> Законопроект «О высокоавтоматизированных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации» // Федеральный портал проектов нормативных правовых актов. URL: <https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=116763> (дата обращения: 28.02.2024).

<sup>18</sup> Законопроект «О высокоавтоматизированных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации» // Федеральный портал проектов нормативных правовых актов. URL:

Концептуальная проблема перечисленных законопроектов видится в смещении частноправовых и публично-правовых средств регулирования, а также в перегруженности текста техническими нюансами.

Оценивая перспективы подготовки нового законопроекта с чистого листа, отметим следующее. В российской технике законотворчества для достижения цели урегулирования той или иной сферы общественных отношений нередко используется практика принятия закона, регулирующего не всю сферу целиком, а только основы или принципы. Например, федеральный закон «Об общих принципах организации местного самоуправления в Российской Федерации»<sup>19</sup>, федеральный закон «Об общих принципах организации публичной власти в субъектах Российской Федерации»<sup>20</sup> или федеральный закон «Об основах охраны здоровья граждан в Российской Федерации»<sup>21</sup>.

Представляется, аналогичный законодательный приём применим для урегулирования и сферы автономных транспортных средств – принятие федерального закона с возможным наименованием «Об основах правового режима автономных транспортных средств».

Новый закон должен быть направлен на формирование системы принципов правового регулирования соответствующей отрасли, главным из которых должен стать принцип безопасности эксплуатации автономного транспортного средства.

Видится необходимым тщательная проработка внутреннего деления на разделы, каждый из которых должен быть подчинён какой-либо идее или принципу. Именно за счёт внедрения подобной рубрикации можно эффективно отделить публично-правовые и частноправовые средства регулирования.

Конкретизация наполнения проекта федерального закона «Об основах правового режима автономных транспортных средств» является перспективным направлением для будущего научного поиска и доктринальных исследований.

Двигаясь далее по иерархии нормативно-правовых актов, укажем, что на уровне подзаконных актов регулирование ведётся посредством установления экспериментальных правовых режимов. В 2022 г. Правительством РФ было принято три постановления, вводящих такие режимы<sup>22</sup>.

---

<https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=116763> (дата обращения: 28.02.2024).

<sup>19</sup> Федеральный закон от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» // Российская газета. 2003. № 202.

<sup>20</sup> Федеральный закон от 21.12.2021 № 414-ФЗ «Об общих принципах организации публичной власти в субъектах Российской Федерации» // Российская газета. 2021. № 294.

<sup>21</sup> Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Российская газета. 2011. № 263.

<sup>22</sup> Постановление Правительства РФ от 09.03.2022 № 309 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств» // Собрание законодательства РФ. 2022. № 12. Ст. 1817; Постановление Правительства РФ от 17.10.2022 № 1849 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере



Как следует из федерального закона «Об основных требованиях в Российской Федерации», смысл экспериментального правового режима состоит во введении *специального* правового регулирования на определённой территории или в отношении определённой группы лиц (ст. 13)<sup>23</sup>. Думается, что само по себе решение Правительства урегулировать использование автономных транспортных средств посредством подобного временного режима вполне оправдано, подразумевая, что соответствующие подзаконные акты рассматриваются в качестве предпосылки к принятию полноценного федерального закона.

По итогам проведённого анализа представляется возможным сделать вывод, что системное регулирование использования автономных транспортных средств пока что не достигнуто.

Предыдущие законотворческие инициативы представляют собой важные импульсы в данной сфере правового регулирования, но окончательных целей пока не достигли.

Объективно необходимым видится разработка и последующее принятие *специального* федерального закона, который должен стать концептуальной основой регулирования различных вопросов, в том числе вопросов технического характера.

### Список литературы

1. Беляева Г. С. Правовой режим: понятие и признаки // Вестник РУДН. Серия: Юридические науки. 2021 Т. 25. № 1. 281–293.
2. Вавилин Е. В. Беспилотные транспортные средства: от терминологии к новым правовым режимам // Хозяйство и право. 2023. № 8. С. 3–21.
3. Гоц Е. В. Вопросы публично-правового регулирования общественных отношений, связанных с внедрением инновационных транспортных средств в России: историко-правовой анализ // Транспортное право. 2023. № 4. С. 7–10.
4. Дремлюга Р. Ю., Яковенко А. А. Регулирование тестирования беспилотного автотранспорта: опыт Европы // Азиатско-тихоокеанский регион: экономика, политика, право. 2020. № 1. С. 103–117.
5. Сергеев А. М., Демченко М. В. Субъектный состав правоотношений, возникающих при использовании инновационных (беспилотных) транспортных

---

цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств в отношении реализации инициативы "Беспилотные логистические коридоры" на автомобильной дороге общего пользования федерального значения М-11 "Нева"» // Собрание законодательства РФ. 2022. № 43. Ст. 7409; Постановление Правительства РФ от 29.12.2022 № 2495 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по предоставлению транспортных услуг с использованием высокоавтоматизированных транспортных средств на территориях отдельных субъектов Российской Федерации» // Собрание законодательства РФ. 2023. № 1. Ст. 300.

<sup>23</sup> Федеральный закон от 31.07.2020 № 247-ФЗ «Об обязательных требованиях в Российской Федерации» // Российская газета. 2020. № 171.

средств в предпринимательской деятельности // Проблемы экономики и юридической практики. 2024. Т. 20. № 1. С. 64–69. DOI: 10.33693/2541-8025-2024-20-1-64-69.

**Alexey M. Sergeev**

Postgraduate student

Department of Legal Regulation of Economic Activities,  
Financial University under the Government of the Russian Federation.  
(Moscow, Russian Federation)  
alexei\_sergeev@mail.ru

## **SOURCES OF LEGAL REGULATION OF THE USE OF INNOVATIVE VEHICLES**

**Abstract:** The present article is devoted to the analysis of the systematic nature of legal regulation of the use of autonomous vehicles. The author considers the prospects for the development of sources of such regulation. The absence of international law in this area is emphasized, and the adoption of any international legal agreements or conventions seems unpromising. It is pointed out that the Constitution of the Russian Federation contains the necessary basis for the regulation of scientific and technological progress in the sphere of autonomous vehicles. The recent Presidential Decree on National Development Goals (No. 309) is expected to herald broad legislative and doctrinal interest. No federal law regulating the use of autonomous vehicles has been adopted in Russia to date. The author examines the conceptual problems of earlier legislative initiatives. Taking into account the shortcomings of previous draft laws, a general idea of a law with a possible title «On the Fundamentals of the Legal Regime of Autonomous Vehicles» is proposed

**Keywords:** unmanned vehicles, innovative vehicles, autonomous vehicles, highly automated vehicles, legal regimes, sources of law.

**Хамидуллин Руслан Сибгатуллович**

Кандидат юридических наук, доцент кафедры криминалистики,  
Уральский государственный юридический  
университет имени В. Ф. Яковлева  
(г. Екатеринбург, Российская Федерация)  
sledgsugu@mail.ru

## **КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА**

**Аннотация:** Предметом исследования являются возможности использования систем искусственного интеллекта в целях раскрытия и расследования преступлений. Автор на примере GPT (Generative Pre-trained Transformer) архитектуры нейросети, придуманной исследователями Google, показывает возможности искусственного интеллекта по анализу ситуаций, возникающих в ходе раскрытия и расследования преступлений, и выдвижению на их основе обоснованных версий по обстоятельствам совершения противоправного деяния. В ходе исследования демонстрируется возможность на основе таких версий составлять программы (планы) расследований. Особое внимание уделяется процессу обучения нейросети использовать современные криминалистические средства и методы в выявлении, раскрытии и расследовании преступлений.

**Ключевые слова:** криминалистическое обеспечение, нейросеть, искусственный интеллект, выявление, раскрытие, расследование, преступления, административные правонарушения, следователь, оперуполномоченный, прокурор.

Использование искусственного интеллекта в раскрытии и расследовании преступлений представляет собой значительный прогресс в области криминалистики. Эта технология позволяет изменить традиционные методы работы правоохранительных органов, обогатив их арсенал инструментов. Криминалистические аспекты применения искусственного интеллекта включают анализ больших объёмов данных, распознавание образов, автоматизированную обработку доказательств и прогнозирование совершения новых преступлений. Электронно-цифровое обучение позволяет создавать модели, способные выявлять закономерности в криминальных событиях, определять характеристики потенциальных преступников и выявлять ключевые факторы, влияющие на динамику ситуации в этом контексте.

Однако следует учитывать этические и юридические аспекты применения искусственного интеллекта в криминалистике, такие как прозрачность алгоритмов, сохранение конфиденциальности данных и предотвращение

возможных проблем с принятием решений. В этой работе будет рассмотрено, как использование искусственного интеллекта влияет на эффективность и надёжность раскрытия и расследования преступлений, а также каким вызовам и перспективам подвержен этот процесс в контексте криминалистической деятельности.

Искусственный интеллект способствует улучшению качества работы правоохранительных органов путём автоматизации рутинных операций и анализа данных. Системы машинного обучения могут быстро обрабатывать огромные объёмы информации, выявляя скрытые связи между различными событиями и лицами, что значительно ускоряет процесс расследования<sup>1</sup>.

Согласно Национальной стратегии развития искусственного интеллекта на период до 2030 г. (Указ Президента РФ от 10.10.2019 № 490 О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»)), под таковым подразумевается комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе то, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений.

Важными аспектами, которые следует учитывать при применении систем искусственного интеллекта, являются, прежде всего, обеспечение защиты конституционных прав и свобод человека и гражданина. Это касается и права каждого человека на неприкосновенность его частной жизни. Необходимо также подчеркнуть недопустимость использования искусственного интеллекта с целью нанесения умышленного вреда гражданам и юридическим лицам.

Другой значимый аспект состоит в предупреждении и минимизации рисков, которые могут возникнуть в результате использования технологий искусственного интеллекта. В связи с этим важно организовать работу алгоритмов искусственного интеллекта таким образом, чтобы они были открытыми и понятными. Это позволит контролировать процесс достижения результатов и предотвратить возможные негативные последствия<sup>2</sup>.

В свете повышенного уровня преступности, применения преступниками новых методов и средств совершения преступлений, а также недостаточно эффективных показателей раскрываемости, становится необходимо открывать

---

<sup>1</sup> Тарасов А. В., Темзоков А. В. Криминалистические аспекты использования искусственного интеллекта в раскрытии и расследовании преступлений // Теория и практика общественного развития. 2023. № 10. С. 256–261.

<sup>2</sup> Колычева А. Н. Перспективы внедрения искусственного интеллекта в раскрытие и расследование преступлений // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2022. № 3. С. 172–177.

новые пути совершенствования деятельности, связанной с выявлением, раскрытием и расследованием преступлений. Недостаточно эффективная система показателей, низкий уровень подготовки правоприменителей, дальнейшая бюрократизация следственной и судебной системы, подчинённость субъектов расследования, коррупционные риски уголовно-процессуальной деятельности и непосредственно уголовно-процессуального законодательства и ряд других факторов негативно сказываются на качестве данной деятельности. Ключевую роль в изменении сложившейся ситуации играют интеллектуальные возможности отдельных сотрудников правоохранительных органов, следователей, оперативных сотрудников, прокуроров, а также руководителей этих структур. Однако данный подход оказывается недостаточным для кардинального перелома в сложившейся обстановке. В этой связи становится необходимо разработать качественно новую систему интеллектуального обеспечения оперативно-розыскной, криминалистической и уголовно-процессуальной деятельности, включая в них применение систем искусственного интеллекта.

Искусственный интеллект представляет собой неотъемлемый атрибут в современной и эффективной оперативно-розыскной и уголовно-процессуальной деятельности, а не фактор, приводящий к исключению человеческого элемента. Система интеллектуального обеспечения уголовного процесса должна включать в себя следующие взаимосвязанные и взаимодополняющие элементы:

- подготовка сотрудников, занимающихся выявлением, раскрытием и расследованием преступлений;
- законодательное обеспечение уголовного процесса;
- научно-исследовательское обеспечение уголовно-процессуальной деятельности;
- информационно-техническое обеспечение уголовного судопроизводства;
- использование систем искусственного интеллекта в уголовном процессе, криминалистике и оперативно-розыскной деятельности.

При этом внедрение систем искусственного интеллекта открывает перспективу для успешного развития уголовного судопроизводства<sup>3</sup>.

На наш взгляд наиболее важным элементом в раскрытии и расследовании преступлений с использованием искусственного интеллекта является криминалистическое обеспечение такой деятельности.

Отметим, что в данном исследовании под криминалистическим обеспечением раскрытия и расследования преступлений путём использования искусственного интеллекта следует понимать совокупность знаний и навыков субъектов раскрытия и расследования преступлений по эффективному использованию систем искусственного интеллекта в решении служебных задач правоохранительной деятельности.

---

<sup>3</sup> Афанасьев А. Ю. Искусственный интеллект или интеллект субъектов выявления, раскрытия и расследования преступлений: что победит? // Библиотека криминалиста. 2018. № 3. С 28–34

В настоящее время криминалистическое обеспечение раскрытия и расследования преступлений становится всё более актуальной и сложной задачей для правоохранительных органов. Сложность заключается в необходимости анализировать большие объёмы информации, выявлять скрытые связи и паттерны, а также прогнозировать возможные сценарии развития дела. В связи с этим использование искусственного интеллекта (ИИ) может стать эффективным инструментом для улучшения результатов расследования.

Одним из примеров применения ИИ в криминалистике является использование GPT (Generative Pre-trained Transformer). GPT – это модель искусственного интеллекта, которая обучается на больших объёмах текстовых данных и способна генерировать связные ответы на заданные вопросы или предоставленные материалы.

В рамках проведённого исследования осуществлено обучение GPT на материалах, которые предлагаются студентам, изучающим курс криминалистики в высших учебных заведениях. В чат GPT были предоставлены задачи и информация, необходимая для их решения. ИИ эффективно и точно давал ответы, предлагая гипотезы, составляя программы и алгоритмы действий, необходимые для раскрытия и расследования преступлений на различных этапах.

Для проверки эффективности GPT в реальных условиях мы провели эксперимент с использованием материалов уголовного дела, находящегося в производстве Главного следственного управления ГУ МВД России по Свердловской области. В чат GPT были представлены материалы дела, и на основе этой информации ИИ выдвигал версии и разрабатывал программу расследования на начальном этапе. После этого, предложенные действия и мероприятия GPT были сравнены с действиями, проводимыми следователями и оперуполномоченными в рамках реального расследования.

Результаты эксперимента показали, что искусственный интеллект, представленный GPT, способен детально и объективно анализировать и планировать мероприятия, необходимые для раскрытия и расследования преступлений. Он также может помочь в формировании вопросов для экспертизы и определении различных видов экспертиз. Это позволяет сделать вывод о возможности эффективного использования искусственного интеллекта в правоохранительной деятельности не только для раскрытия преступлений, но и для предотвращения их совершения, определения обстоятельств и места преступления.

Однако, необходимо отметить, что использование искусственного интеллекта в криминалистическом обеспечении имеет свои ограничения. Во-первых, ИИ не обладает человеческим интуитивным пониманием и эмоциональным опытом, что может сказаться на точности его выводов. Во-вторых, ИИ может быть подвержен ошибкам, особенно если обучение проводилось на неполных или некорректных данных.

Тем не менее, при правильном применении искусственный интеллект может стать ценным инструментом для криминалистического обеспечения

раскрытия и расследования преступлений. Он может значительно ускорить процесс анализа информации и организовать планирование расследования на различных его этапах. В результате использование искусственного интеллекта может повысить эффективность работы правоохранительных органов и улучшить качество расследования преступлений.

### **Список источников**

1. Афанасьев А. Ю. Искусственный интеллект или интеллект субъектов выявления, раскрытия и расследования преступлений: что победит? // Библиотека криминалиста. 2018. № 3. С 28–34.
2. Колычева А. Н. Перспективы внедрения искусственного интеллекта в раскрытие и расследование преступлений // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2022. № 3 С. 172–177.
3. Тарасов А. В., Темзоков А. В. Криминалистические аспекты использования искусственного интеллекта в раскрытии и расследовании преступлений // Теория и практика общественного развития. 2023. № 10. С. 256–261.

### **Ruslan K. Sibagatulovich**

Candidate of Law, Associate Professor of the Department of Criminalistics  
Ural State Law University named after V. F. Yakovlev  
(Yekaterinburg, Russian Federation)  
sledgsugu@mail.ru

## **FORENSIC SUPPORT OF DISCLOSURE AND INVESTIGATION OF CRIMES USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES**

**Abstract:** The subject of the study is the possibility of using artificial intelligence systems for the purpose of solving and investigating crimes. Using the example of GPT (Generative Pre-trained Transformer), a neural network architecture invented by Google researchers, the author shows the capabilities of artificial intelligence to analyze situations that arise during the detection and investigation of crimes and, based on them, put forward reasonable versions of the circumstances of the commission of an illegal act. The study demonstrates the possibility of drawing up programs (plans) for criminal investigations based on such versions. The object of the study is the social relations that arise during the use of artificial intelligence systems in law enforcement. Particular attention is paid to the process of training a neural network to use modern forensic tools and methods in detection, detection and investigation.

**Keywords:** forensic support, neural network, artificial intelligence, detection, disclosure, investigation, crimes, administrative offenses, investigator, detective, prosecutor.

**Цветкова Анна Денисовна**  
Младший научный сотрудник  
АНО «Центр содействия развитию криминалистики «КримЛиб»»,  
Уральский государственный юридический  
университет имени В. Ф. Яковлева  
(г. Екатеринбург, Российская Федерация)  
at@crimlib.info

## **ПРОБЛЕМНЫЕ АСПЕКТЫ ОПРЕДЕЛЕНИЯ ИСПОЛНИТЕЛЯ НАПЕЧАТАННОГО ТЕКСТА\***

**Аннотация:** При работе с электронными текстами, которых в нашей жизни становится всё больше, следствие может столкнуться с ситуацией, когда автороведческая экспертиза не позволяет сделать вывод об исполнителе напечатанного текста. Для решения этой проблемы юридическим науке и практике следует обратить внимание на феномен клавиатурного почерка, отвечающего за индивидуальные особенности набора текста на клавиатуре.

**Ключевые слова:** почерковедческая экспертиза, автороведческая экспертиза, клавиатурный почерк, исполнитель текста, электронный документооборот.

Одной из традиционных и весьма актуальных задач криминалистики является определение исполнителя того или иного текста. Важность данного вопроса обусловлена большим количеством документов в нашей жизни – по меткому замечанию советского поэта В. И. Лебедева-Кумача: «без бумажки ты – букашка, а с бумажкой – человек». При этом и подлог документов, и отрицание факта причастности к созданию определённого текста достаточно часто встречаются в следственной и судебной практике. Проверка указанных фактов осуществляется с помощью почерковедческой и автороведческой экспертиз, причём нередко эти исследования проводятся комплексно с целью взаимной проверки результатов, хотя каждое из них имеет свою специфику.

Почерковедческая экспертиза исследует письменно-двигательные навыки и их внешние проявления: сила нажатия, наклон букв, выработанность почерка, связность, конфигурация полей и строк, относительное размещение точек и т. д.<sup>1</sup>

---

\* Исследование выполнено за счет гранта Российского научного фонда № 23-78-10011, <https://rscf.ru/project/23-78-10011/>.

<sup>1</sup> Антропов А. В., Бахтеев Д. В., Кабанов А. В. Криминалистическая экспертиза: учеб. пособие для бакалавриата, специалитета и магистратуры. М.: Издательство Юрайт, 2018. С. 99–107.



Автороведческие исследования сосредотачиваются на признаках письменной речи: лексика, словарный запас, логика текста, особенности речевых оборотов и построения предложений и т. д.<sup>2</sup>

В большинстве случаев данные экспертизы взаимозаменяемы, поскольку рукописные тексты чаще создаются в форме свободного изложения (школьные сочинения, контрольные работы или экзамены в университете, объяснительные, служебные записки и разного рода заявления, предсмертные записки), когда в равной мере проявляются авторский стиль и индивидуальные признаки почерка пишущего человека.

Однако возможны ситуации, когда автором и исполнителем текста являются разные лица: например, если некто записывает под диктовку, дублирует написанное ранее иным человеком, создаёт шаблонный формальный документ (например, расписку о получении денежных средств в качестве займа). В этом случае автороведческая экспертиза оказывается ненужной, а исследование признаков письменной речи, описывающих общую грамотность, стилистику речи и другие авторские черты текста, в рамках почерковедческой экспертизы<sup>3</sup> представляется бесполезным. Отдельным направлением, где почерковедческая экспертиза становится незаменимой, является криминалистическое исследование подписи – малого по объёму и наиболее трудного для идентификации объекта данного вида экспертиз<sup>4</sup>, не несущего в себе никаких сведений об авторе, но подделываемого очень часто.

Обратная ситуация тоже вполне возможна: когда не так важен исполнитель, как автор – то есть лицо, ответственное за идею определённого текста (например, экстремистского содержания). В подобных обстоятельствах анализировать почерковый материал не так значимо (особенно, если исполнитель достоверно известен), как проводить автороведческие исследования.

Таким образом, несмотря на кажущуюся близость двух направлений судебной экспертизы, они решают уникальные задачи, которые не перекрываются в ряде случаев. Это же актуально и в современных условиях.

Так, всё больше текстового (документарного или бездокументарного) взаимодействия происходит в цифровой среде. Российское государство проводит политику всеобщего перехода на электронный документооборот: развиваются сервисы электронного правительства (так, например, в 2022–2023 годах на портале Госуслуг добавились функции, позволяющие с его помощью предъявлять водительское удостоверение и свидетельство транспортного средства (СТС), подавать заявления на расторжение брака, на получение единого

---

<sup>2</sup> Антропов А. В., Бахтеев Д. В., Кабанов А. В. Криминалистическая экспертиза: учеб. пособие для бакалавриата, специалитета и магистратуры. М.: Издательство Юрайт, 2018. С. 127.

<sup>3</sup> Бобовкин М. В. [и др.] Судебно-почерковедческое и технико-криминалистическое исследование документов: практическое пособие / отв. ред. М. В. Бобовкин, А. А. Проткин. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2023. С. 25–32.

<sup>4</sup> Бахтеев Д. В. Особенности распознавания подлога подписи человеком как первичные критерии для разработки системы искусственного интеллекта // Сибирское юридическое обозрение. 2020. Т. 17. № 4. С. 519.

пособия семьям с детьми и т. д.); вводится кадровый электронный документооборот (на федеральном уровне посредством онлайн-платформы «Работа в России»), Гражданский кодекс приравнял электронные документы к письменной форме сделок. Одновременно с этим межличностное общение во многом стало осуществляться посредством мессенджеров и социальных сетей, причём вместо постоянных звонков, которые предсказывались в 1990-х, доминируют письменные формы коммуникации. Учебная и научная деятельность также осуществляется сейчас в цифровой среде – единицы учёных всё ещё пишут свои статьи от руки, большинство же даже пожилых деятелей науки творят с помощью текстовых редакторов.

Продолжать данный перечень можно долго, однако уже из приведённого очевидно, какое значимое место в нашей повседневной жизни заняли электронные тексты, созданные различными людьми. В связи с этим вполне закономерно, что во многих преступных деяниях (совершавшихся ранее или новых – компьютерных) используются электронные тексты (документарные и бездокументарные) для: согласования вопросов незаконного сбыта изъятых или ограниченных в обороте вещей; поиска соучастников и (или) средств совершения преступлений; подлога служебных документов; фальсификации доказательств и т. п. – список почти неограничен. Таким образом, перед криминалистикой и судебной экспертизой встаёт новая задача – определить исполнителя напечатанного текста.

Сегодня решение данной проблемы осуществляется только посредством автороведческой экспертизы: например, если речь идёт о сговоре на незаконный сбыт и приобретение наркотических средств в переписке на закрытом форуме, и подозреваемый отрицает свою причастность к данному преступлению, то сопоставляются особенности его сетевого общения в легальных обстоятельствах (переписка с девушкой, начальником и т. п.) и признаки письменной речи, обнаруженные в спорных сообщениях противоправного характера.

Однако, как и при работе с рукописными текстами, для печатных материалов могут возникать ситуации, когда автороведческая экспертиза не способна дать ответ на вопрос об исполнителе. В этом случае прибегают к презумпции, согласно которой исполнителем напечатанного текста является собственник персонального компьютера или аккаунта, с которого соответствующий текст создавался. При этом весьма очевидна порочность данной презумпции: даже в одной семье обычно у всех членов имеется доступ к компьютерам друг друга, не говоря уже о корпоративных (например, установленных в коммерческой организации или вузе) и публичных (предоставляемых посетителям библиотек, к примеру) устройствах. Данное обстоятельство порождает актуальную проблему отсутствия приемлемых механизмов для достоверной идентификации исполнителя напечатанного текста, так как какой-то аналог почерковедческой экспертизы в данной ситуации не применим – нет отражения индивидуальных навыков печати в итоговом тексте на экране.

Однако специфика при наборе текста у разных людей всё же наблюдается – разнятся такие показатели как:

- динамика ввода (промежуток времени с момента начала нажатия на одну клавишу до момента начала нажатия на следующую);
- сила давления на клавиши клавиатуры;
- скорость ввода (общее число символов, набираемое за единицу времени);
- темп печати (число символов единого смыслового элемента (без отрыва от клавиатуры), набранное за единицу времени);
- выработанность печатно-двигательного навыка (рассчитываемая в зависимости от числа используемых пальцев, скорости печати и числа допускаемых ошибок);
- характер наложений (расположение ладоней над клавиатурой и разграничение «зон ответственности» пальцев);
- устойчивые паттерны (проявляющиеся в использовании сочетаний «горячих клавиш», служебных функций компьютера, особенностей набора отдельных символов, таких как «№», «'»», «ё» и др.);
- системные опечатки;
- модель внесения исправлений (например, стирает ли человек напечатанное после допущенной ошибки, чтобы переписать всё заново, или переходит на место опечатки курсором, чтобы исправить непосредственно только её)<sup>5</sup>.

Совокупность перечисленных характеристик образует уникальный навык каждого печатающего человека – его клавиатурный почерк, исследуемый на сегодняшний день, главным образом, специалистами компьютерно-технических областей знания. Ими же разрабатываются системы (программные и программно-аппаратные комплексы), позволяющие зафиксировать отдельные из перечисленных выше характеристик, – так называемые кейлоггеры<sup>6</sup>. Указанные системы встраиваются в клавиатуру или подключаются как внешние носители и записывают все нажатия на клавиши. Некоторые из них формируют с настроенной регулярностью отчёт, который может быть воспринят и проанализирован человеком, и сохраняют его во встроенной памяти (программно-аппаратные системы) или направляют на указанный в момент установки адрес электронной почты (программные сервисы). Однако большая часть подобных модулей на сегодняшний день используется в целях личной безопасности (настройка двухфакторной аутентификации для доступа к компьютеру или отдельным материалам на нём) или коммерческих интересах

---

<sup>5</sup> Перегудов А. В. Анализ клавиатурного почерка. Способы его применения // *Interactive science*. 2018. №6 (28). С. 60; Аверин А. И., Сидоров Д. П. Аутентификация пользователей по клавиатурному почерку // *Огарёв-Online*. 2015 С. 4.

<sup>6</sup> Cormac Herley, Dinei Florencio. How To Login From an Internet Cafe Without Worrying About Keyloggers // MSR-TR-2006-12. July 2006. URL: <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/soups06.pdf>.

(разработка ориентированных на пользователей клавиатур или промышленный шпионаж).

Представляется, что юридической науке в целом и криминалистке в частности тоже пришло время обратить внимание на феномен клавиатурного почерка с тем, чтобы разрешить следующие проблемные аспекты:

1) Определить с юридико-правовой точки зрения природу клавиатурного почерка – в частности, его место в системе персональных данных.

2) Раскрыть природу данного феномена с позиций криминалистики (выявить наиболее стабильные, воспроизводимые и индивидуальные признаки из перечисленных выше).

3) Сделать возможным получение свободных образцов клавиатурного почерка; в ситуации централизованного сбора их на государственном уровне – сформулировать требования к базе данных, где будут храниться сведения о нём.

4) Выделить критерии, которыми должны обладать сведения о клавиатурном почерке, чтобы было возможным признать их в качестве доказательственных материалов<sup>7</sup>.

5) Разработать соответствующую экспертную методику.

Ответы на поставленные вопросы и работа по указанным направлениям в тандеме со специалистами в области компьютерных технологий позволят юристам разрешить практическую задачу определения исполнителя напечатанного текста, которая, как признают сотрудники правоохранительных органов, стоит весьма остро, а также обогатить науку новым направлением криминалистических исследований.

### Список литературы

1. Аверин А. И., Сидоров Д. П. Аутентификация пользователей по клавиатурному почерку // Огарёв-Online. 2015 С. 1–5.

2. Антропов А. В., Бахтеев Д. В., Кабанов А. В. Криминалистическая экспертиза: учеб. пособие для бакалавриата, специалитета и магистратуры. М.: Издательство Юрайт, 2018. 184 с.

3. Бахтеев Д. В. Особенности распознавания подлога подписи человеком как первичные критерии для разработки системы искусственного интеллекта // Сибирское юридическое обозрение. 2020. Т. 17. № 4. С. 514–522.

4. Бобовкин М. В. [и др.] Судебно-почерковедческое и технико-криминалистическое исследование документов: практическое пособие / отв. ред. М. В. Бобовкин, А. А. Проткин. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2023. 286 с.

5. Перегудов А. В. Анализ клавиатурного почерка. Способы его применения // Interactive science. 2018. №6 (28). С. 59–64.

---

<sup>7</sup> Федоров И. З. К вопросу о расширении источников сведений, допускаемых в качестве доказательств по уголовному делу // Вестник Российского университета кооперации. 2015. № 4 (22). С. 142–145.

6. Федоров И. З. К вопросу о расширении источников сведений, допускаемых в качестве доказательств по уголовному делу // Вестник Российского университета кооперации. 2015. № 4 (22). С. 142–145.

7. Cormac Herley, Dinei Florencio. How To Login From an Internet Cafe Without Worrying About Keyloggers // MSR-TR-2006-12. July 2006. URL: <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/soups06.pdf>.

**Anna D. Tsvetkova**

Junior Researcher

Centre for Assistance to the Development of Forensic Science «CrimLib»,  
Ural State Law University named after V. F. Yakovlev  
(Yekaterinburg, Russian Federation)  
at@crimlib.info

### **PROBLEMATIC ASPECTS OF IDENTIFYING THE EXECUTOR OF A PRINTED TEXT**

**Abstract.** While dealing with electronic texts which are becoming more and more common in our lives investigators may encounter situations when forensic examination of texts fails to identify the executor of the printed text. To solve this problem, legal science and practice should pay attention to the phenomenon of keystroke dynamics which is responsible for the individual characteristics of typing on the keyboard.

**Keywords:** handwriting expertise, forensic analysis, keystroke dynamics, executor of the text, electronic document flow.

**Шевырталов Егор Павлович**  
Адъюнкт,  
Уральский юридический институт МВД России  
(г. Екатеринбург, Российская Федерация)  
shevyrtalove@yandex.ru

## **СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ОБРАБОТКИ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМЫЕ ПРИ РАССЛЕДОВАНИИ КРАЖ И УГОНОВ АВТОМОБИЛЕЙ**

**Аннотация:** В данной статье речь пойдёт лишь о некоторых возможностях использования современных технологий обработки информации и путях их развития для эффективного решения задач, стоящих перед органами внутренних дел. Автором статьи выделяются несколько перспективных направлений совершенствования процесса расследования краж и угонов автомобилей. Первое – интеграция беспилотных летательных аппаратов в работу СПО «Паутина». Второе – автоматизация интерпретации информации, полученной в ходе получения информации о соединениях между абонентами и (или) абонентскими устройствами.

**Ключевые слова:** информационные технологии, кражи автомобилей, угоны автомобилей, СПО «Паутина», БПЛА, абонентские соединения.

Обеспечение сохранности имущества, в том числе личного автотранспорта, безусловно задача собственника, однако кражи и угоны автомобилей занимают значительное место в структуре преступности. Так, только за 2023 год было зарегистрировано 3 782 кражи автомобиля<sup>1</sup>. В каждом случае перед сотрудниками Министерства внутренних дел Российской Федерации (далее МВД России) стоит задача по розыску похищенного или угнанного транспортного средства, а также по установлению лица, совершившего преступление. В этом могут помочь современные технологии обработки информации, так как научно-технический прогресс открывает перед правоохранительными органами широкие возможности для эффективного расследования различных видов преступлений, в том числе краж и угонов автомобилей.

С 2022 года на всей территории России, за исключением четырёх новых субъектов, функционирует специальное программное обеспечение «Паутина» (далее СПО «Паутина»), аккумулирующее всю информацию с дорожных камер фото-, видеофиксации на единой платформе – Центр автоматизированной фиксации административных правонарушений в области дорожного движения

---

<sup>1</sup> Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года // Министерство внутренних дел Российской Федерации [Электронный ресурс]. 20 января 2024. URL: <https://clck.ru/3BHzWG> (дата обращения: 02.05.2024).

(далее ЦАФАП). Возможности «Паутины» не ограничиваются регистрацией административных правонарушений. Данная технология является классическим примером «Big Data» (от англ. big data – большие данные), где программный анализ и структурирование полученных сведений в автоматическом режиме позволяет выявлять «двойников»<sup>2</sup>, водителей с опасным вождением, а также факты слежки за конкретным автомобилем. Одной из основных функций данной системы является розыск транспортных средств. По запросу сотрудников МВД России им из «Паутины» предоставляются данные о времени и месте проезда, а также направлении движения авто. Сведения сопровождаются изображениями с камеры фото-, видеофиксации, на которых можно рассмотреть не только автомобиль, но и лиц, находящихся в транспортном средстве<sup>3</sup>. В тех случаях, когда объект попадает в зоны фиксации нескольких камер, СПО «Паутина» создаёт маршрут с картой передвижений разыскиваемого автомобиля. Трудно переоценить важность такой информации для установления местонахождения имущества, оказавшегося в руках преступника.

По-нашему мнению, перспективным направлением развития систем мониторинга за дорожным движением является интеграция камер видеонаблюдения, расположенных на беспилотных летательных аппаратах (далее БПЛА), в работу СПО «Паутина».

Во многих субъектах России на вооружении Госавтоинспекции МВД России (далее ГАИ) стоят БПЛА, фиксирующие нарушение правил дорожного движения. Они используются при контроле дорог, где наиболее часто происходят дорожно-транспортные происшествия, с целью предотвращения аварийных ситуаций и выявления водителей, совершающих запрещённые на данном участке маневры, например выезд на встречную полосу движения с пересечением сплошной линии<sup>4</sup>. В условиях большой территории нашей страны, с высоким количеством загородных трасс, применение БПЛА приобретает актуальный характер.

На данный момент в отличие от стационарных комплексов фото-, видеофиксации нарушений ПДД, работающих в автоматическом режиме, БПЛА выступают только инструментом видеофиксации правонарушений, а привлечение лица к ответственности происходит по стандартной процедуре. Выглядит это следующим образом: оператор посредством систем управления БПЛА фиксирует факт административного правонарушения и передаёт информацию ближайшему посту ДПС, после чего сотрудники ГАИ останавливают автомобиль и составляют необходимый административный протокол. В итоге, записанное с высоты птичьего полёта видео используется как

---

<sup>2</sup> Двойник – автомобиль, идентификационные признаки которого полностью совпадают с законно купленным и поставленным на учёт ТС.

<sup>3</sup> Демишева Е. Тотальная слежка, штрафы и розыск нарушителей: как устроена «Паутина» // Auto.ru. Журнал [Электронный ресурс]. 31 октября 2022. URL: <https://clck.ru/3BNHzdy> (дата обращения: 04.05.2024).

<sup>4</sup> Гронский Я. «Удивлялись, но только сначала». Как беспилотники ГИБДД ловят нарушителей // AUTONEWS [Электронный ресурс]. 11 января 2022. URL: <https://clck.ru/3BNzhQ> (дата обращения: 05.05.2024).

приложение к протоколу об административном правонарушении.

Однако возможности применения БПЛА в деятельности ГАИ не должны ограничиваться использованием видеозаписи лишь для подтверждения факта нарушения ПДД. Передача информации, полученной с камер БПЛА, в ЦАФАП и её последующая обработка посредством СПО «Паутина» позволит вывести на новый уровень работу правоохранительных органов. Во-первых, можно не только фиксировать, но и выявлять административные правонарушения в области безопасности дорожного движения, а также в автоматическом режиме выносить постановления о привлечении лица к административной ответственности. Во-вторых, анализ данных о времени, дате и точном местоположении БПЛА, зафиксировавшего разыскиваемый автомобиль, станет базой для обоснованного предположения о примерном местонахождении данного транспортного средства. Такие сведения, несомненно, окажут помощь в расследовании краж и угонов автомобилей.

Однако для достижения этого необходимо решить ряд задач:

1) Внедрить в камеры фото-, видеофиксации, установленные на БПЛА, функционал по идентификации транспортного средства посредством его индивидуальных признаков: государственному регистрационному номеру, марке, модели, цвету, типу кузова и т. д. Это даст возможность анализировать транспортные потоки, обнаруживать в плотном трафике искомый автомобиль и, при необходимости, вести наблюдение.

2) Объединить стационарные системы фото-, видеофиксации нарушений ПДД и камеры, установленные на БПЛА. Данное техническое решение позволит искусственному интеллекту «Паутины» составлять маршруты движения конкретного автомобиля за определённый период времени.

3) Разработать системы по определению точной скорости транспортного средства в режиме реального времени. Сложность этой задачи заключается в изменчивости кадра, так как БПЛА находится в движении, на него действует сила ветра и сопротивление воздуха, к тому же угол относительно конкретного автомобиля постоянно меняется. Такие особенности «летающих» камер ставят новые задачи для исследователей. В этом контексте внимания заслуживает работа учёных из тихоокеанского островного государства Тонга, которые предложили математическое решение данной проблемы<sup>5</sup>.

4) Увеличение количества БПЛА, состоящих на балансе МВД России. Малое количество БПЛА вынуждает сотрудников ГАИ прибегать к помощи иных государственных органов, например Росгвардии<sup>6</sup>, в результате чего трудно говорить о реализации всех положительных сторон использования БПЛА.

Считаем, что решение вопросов материально-технического обеспечения,

---

<sup>5</sup> Cusack B., Maeakafa G. Establishing effective and economical traffic surveillance in Tonga // The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016. Perth: Edith Cowan University, 2016. P. 53.

<sup>6</sup> Сазонов К. «Поднять шумиху в соцсетях». На службу гаишникам пришли дроны // Газета.ru [Электронный ресурс]. 16 августа 2021. URL: <https://goo.su/CiWir> (дата обращения: 05.05.2024).



связанных с расширением использования БПЛА, не только выведет безопасность дорог России на новый уровень, но и станет дополнительным источником криминалистической информации при расследовании краж и угонов автомобилей.

Таким образом, мы кратко рассмотрели технологию, предоставляющую преимущественно оперативную и криминалистическую информацию, правильное применение которой позволит проводить тактическую операцию по установлению местонахождения разыскиваемого автомобиля. Далее остановимся на следственных действиях, способных оказать содействие в расследовании краж и угонов транспортных средств путём предоставления доказательной информации.

Преступник знает об особенностях российского уголовного законодательства, а именно о том, что преступление, предусмотренное п. «б» ч. 4 ст. 158 УК РФ (кража), является тяжким преступлением, а преступление, предусмотренное ч. 1 ст. 166 УК РФ (угон), – средней тяжести. Поэтому лицо на допросе либо отрицает вину, либо признает её, однако утверждает, что совершил неправомерное завладение, но без цели хищения автомобиля. Таким образом, субъект расследования оказывается в тупике, когда имеется предположение о наличии умысла на хищение, но доказательств, подтверждающих данную следственную версию, нет. Представим следующую следственную ситуацию: задержано лицо по подозрению в совершении кражи автомобиля, при нём обнаружен мобильный телефон с работающей сим-картой, зарегистрированной на задержанного. Что делать в такой ситуации?

Здесь может помочь почти неиспользуемое по уголовным делам изучаемой категории следственное действие, предусмотренное ст. 186.1 УПК РФ, – получение информации о соединениях между абонентами и (или) абонентскими устройствами. С помощью него возможно подтвердить или опровергнуть факты подготовки лица к совершению именно кражи автомобиля, а не его угона. Профессиональные автомобильные воры тщательно подготавливают оружие и средства для хищения, а также подыскивают автомобиль, которым желают завладеть, осуществляют слежку за ним и выбирают наилучшее время для реализации своего умысла<sup>7</sup>. В период совершения таких действий не исключено использование услуг сотовой связи. Оставленные цифровые следы могут служить маркером для проверки тех или иных обстоятельств, на которые ссылается подозреваемый.

Детализация звонков может хоть и косвенно, но подтверждать подготовительную деятельность лица к совершению преступления. Ведь довольно странно на протяжении определённого периода времени находиться в

---

<sup>7</sup> Шевырталов Е. П., Дерюгин Р. А. Современные способы хищения автотранспортных средств // Тенденции развития современного уголовно-процессуального законодательства Российской Федерации: Сборник научных трудов Всероссийской научно-практической конференции, Екатеринбург, 29 апреля 2022 года / Под редакцией Н. С. Расуловой. Екатеринбург: Уральский юридический институт Министерства внутренних дел Российской Федерации, 2022. С. 142–143.

зоне работы базовой станции, в пределах которой также расположен автомобиль, в последующем угнанный проверяемым лицом. Особенно в тех случаях, когда преступник проживает в другом районе и до подготовки к преступлению никогда там не появлялся.

Учёными отмечаются процессуальные и тактические сложности проведения данного следственного действия<sup>8</sup>. Однако наибольшую сложность для правоприменителей представляет последующий анализ полученной от оператора связи информации. Не обладая навыками работы с таблицами звонков абонента и знаниями о принципах работы сотовой связи, становится проблематично определить месторасположение лица в конкретный период времени. Считаем, что возможным решением этой проблемы станет создание специальной программы, способной интерпретировать информацию из таблиц в удобный и понятный вид для любого сотрудника. То есть загружаемые в программу табличные данные должны в автоматическом режиме анализироваться, а также должна создаваться интерактивная карта с геолокациями абонента и адресами базовых станций. Данное программное обеспечение позволит оперативно и с минимальными трудозатратами оптимизировать деятельность правоохранительных органов по расследованию преступлений.

В заключение хочется ещё раз акцентировать внимание на том, что достижения научно-технического прогресса уже сегодня являются эффективными инструментами в борьбе с преступностью. Однако стоит понимать, что любая технология требует постоянного развития. Перед научным сообществом стоит задача по её адаптации к реалиям сегодняшнего дня. Без этой работы невозможно представить рост количества раскрытых преступлений, в том числе по делам, связанным с кражами и угонами автомобилей.

### **Список литературы**

1. Cusack B., Maeakafa G. Establishing effective and economical traffic surveillance in Tonga // The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016. Perth: Edith Cowan University, 2016. Pp. 50–56.
2. Гронский Я. «Удивлялись, но только сначала». Как беспилотники ГИБДД ловят нарушителей // AUTONEWS [Электронный ресурс]. 11 января 2022. URL: <https://clck.ru/3BNzhQ> (дата обращения: 05.05.2024).
3. Демишева Е. Тотальная слежка, штрафы и розыск нарушителей: как устроена «Паутина» // Auto.ru. Журнал [Электронный ресурс]. 31 октября 2022. URL: <https://clck.ru/3BNzdy> (дата обращения: 04.05.2024).
4. Дерюгин Р. А. Криминалистические и процессуальные вопросы производства следственного действия, предусмотренного статьёй 186.1 Уголовно-процессуального кодекса Российской Федерации // Вопросы безопасности. 2016. № 5. С. 43–48.

---

<sup>8</sup> Дерюгин Р. А. Криминалистические и процессуальные вопросы производства следственного действия, предусмотренного статьёй 186.1 Уголовно-процессуального кодекса Российской Федерации // Вопросы безопасности. 2016. № 5. С. 44.

5. Сазонов К. «Поднять шумиху в соцсетях». На службу гаишникам пришли дроны // Газета.ru [Электронный ресурс]. 16 августа 2021. URL: <https://goo.su/CiWir> (дата обращения: 05.05.2024).

6. Шевырталов Е. П., Дерюгин Р. А. Современные способы хищения автотранспортных средств // Тенденции развития современного уголовно-процессуального законодательства Российской Федерации: Сборник научных трудов Всероссийской научно-практической конференции, Екатеринбург, 29 апреля 2022 года / Под редакцией Н. С. Расуловой. Екатеринбург: Уральский юридический институт Министерства внутренних дел Российской Федерации, 2022. С. 141–145.

**Egor P. Shevyrtalov**

Adjunct

Ural Law Institute of the Ministry of Internal Affairs of Russia

(Ekaterinburg, Russian Federation)

shevyrtalove@yandex.ru

## **MODERN INFORMATION PROCESSING TECHNOLOGIES USED IN THE INVESTIGATION OF CAR THEFTS AND CARJACKINGS**

**Abstract:** In this article we will talk only about some possibilities of using modern technologies of information processing and ways of their development for effective solution of tasks facing internal affairs bodies. The author of the article identifies several promising directions for improving the process of investigating car thefts and carjackings. The first is the integration of unmanned aerial vehicles into the work of specialized software «Web». The second – automation of interpretation of information obtained in the course of obtaining information about connections between subscribers and (or) subscriber devices.

**Keywords:** information technologies, car theft, carjacking, specialized software «Web», drone, subscriber connections.

**Щербаков Игорь Олегович**

Преподаватель кафедры криминалистики  
Уральский юридический институт МВД России  
(г. Екатеринбург, Российская Федерация)  
technikk@list.ru

**Ужегов Максим Васильевич**

Курсант факультета подготовки следователей  
Уральский юридический институт МВД России  
(г. Екатеринбург, Российская Федерация)  
uzhegov\_2002@mail.ru

## **ИНТЕРНЕТ ВЕЩЕЙ КАК ИСТОЧНИК КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ**

**Аннотация:** В статье рассматриваются возможности получения необходимой информации с устройств, подключённых к сети Интернет, а также обнаружения цифровых следов преступления и, как результат, формирования доказательств по уголовному делу. Авторы делают акцент на необходимости изучения системы интернета вещей, способов совершения преступлений при помощи методов взлома или любого другого способа влияния на устройство, подключённое к сети Интернет; необходимость уделять наибольшее внимание вопросам криминалистического исследования интернета вещей. Раскрыты вопросы возможности поиска цифровых следов в устройствах, имеющих общий домен, а также установления следов логического и материального характера.

**Ключевые слова:** сеть Интернет, интернет вещей, цифровые следы, криминалистическое исследование, электронные устройства, компьютеризированные системы, умные устройства.

Первая половина 90-ых годов XX века в России была ознаменована появлением сети Интернет, разработка которой как проекта Министерства обороны США началась в 1960 году. Через девять лет была реализована первая связь двух компьютеров (передача между ними сообщений). Датой появления Интернета в России принято считать 7 апреля 1994 года, когда был зарегистрирован первый домен<sup>1</sup>. С этого момента начинается активный процесс цифровизации российского общества и приобщения его к глобальной информационной системе.

В 1999 году британский инженер Кевин Эштон ввёл в оборот термин «Интернет вещей» (англ. Internet of Things, IoT), подразумевая, что, начиная с

---

<sup>1</sup> Арбузова А., Решетникова М. Что такое интернет, кто его придумал и как он устроен: история создания // РБК Тренды [Электронный ресурс]. 15 апреля 2024. URL: <https://trends.rbc.ru/trends/industry/665dace29a7947ea2907e9cc> (дата обращения: 07.05.2024).

XXI века, «соединены» интернетом будут не только люди, но и вещи, различные устройства, например, телефон и компьютер будут подключены к Интернету, причём управлять телефоном можно будет с компьютера или наоборот. И вот в 2009 году происходит так называемый переход от «интернета людей» к «интернету вещей». В 2020 году почти все вещи, которыми пользуется человек, стали взаимодействовать между собой с помощью Интернет-сети, например, робот-пылесос, смартфон, принтер, сканер, стиральная машина, компьютеры, ноутбуки и другие вещи – все они подключены к Интернету и управляются при помощи одного домена (например, смартфона).

Так как все вещи пользователя соединены у одного домена, а также между собой, это значит, что личные данные, а также безопасность некоторых других конфиденциальных данных (пароли, биометрия) находятся в большей уязвимости, так как злоумышленники могут использовать подключённые к доменному серверу устройства и через них взламывать социальные страницы пользователя или, к примеру, банковские приложения. В России на сегодняшний день недостаточно внимания уделяется криминалистическим аспектам исследования интернета вещей, хотя IoT в перспективе является новым способом совершения преступлений. И если преступники уже применяют данный способ для мошенничества и хакерских атак, взлома сайтов и похищений конфиденциальной информации, то правоохранные органы значительно отстают в изучении возможностей криминалистического исследования IoT. Этот факт был высказан учёными Оксфордского университета в 2017 году<sup>2</sup>, но с тех пор мало что изменилось.

В России с 2020-х гг. развивается цифровая криминалистика, появляются приложения для получения необходимой информации, например, Мобильный криминалист, Elcomsoft и другие. Все они используются экспертами для получения доступа к устройству в целях изъятия информации, которая является цифровым следом, что в значительной степени помогает в расследовании преступлений. И несмотря на то, что IoT-системы появились в 2009 году, криминалистические исследования в этой сфере стали развиваться только в 2020-м году. Улучшение и цифровизация технических устройств, окружающих человека, влекут за собой и развитие преступных сообществ. Поэтому изучение возможных способов криминалистического исследования в сфере интернета вещей и возможности изъятия добытой информации, а также использования этих данных в качестве доказательств по уголовному делу является актуальным вопросом на сегодняшний день.

Интернет вещей классифицируют на промышленный и бытовой<sup>3</sup>. Криминалистическим аспектом промышленного применения интернета вещей

---

<sup>2</sup> Smith G. J. D., Moses L. B., Chan J. The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach. *The British Journal of Criminology*. 2017. P. 259–274. DOI: 10.1093/bjc/azw096.

<sup>3</sup> Смушкин А. Б. Отдельные аспекты использования концепции интернета вещей в целях противодействия преступности // *Всероссийский криминологический журнал*. 2020. Т. 14. № 3. С. 453–460. DOI: 10.17150/2500-4255.2020.14(3).453-460.

может являться расследование преступлений, совершённых способами взлома и заражения цифровых устройств вредоносными программами через Интернет. Так, при расследовании преступлений, связанных с промышленным шпионажем или нарушениями экологической безопасности необходимо установить наличие или отсутствие факта взлома программ управляющего центра устройств (т. е. домена, который управляется подключёнными к нему интернет-вещами). Промышленный интернет вещей представляет собой масштабные системы, такие как «умный город», например. Сейчас он применяется в банковской деятельности (служба безопасности банка имеет возможность наблюдать за переводами денежных средств и контролировать ситуации при обмане граждан мошенниками благодаря тому, что банковские карты привязаны к номеру мобильного телефона собственника карты, а все они привязаны к одному блоку центрального управления в отделении банка), в деятельности правоохранительных органов (камеры видеофиксации правонарушений), служб по делам чрезвычайных ситуаций (системы ГЛОНАСС).

Бытовой интернет вещей связан с менее глобальными проектами, такими как «умный дом», умный автомобиль и носимые гаджеты (телефоны, планшеты), которые связаны одной локальной сетью (LAN, Wi-Fi, Bluetooth, NB-IoT).

Отдельное внимание следует уделить вопросам слеδοобследования в процессе совершения преступлений с подобными технически устройствами. Для того, чтобы следователь работал с электронным устройством, ему необходимо иметь представление об этой работе, т. е. понимать, какую информацию можно получить.

В ходе исследования интернета вещей возможно обнаружить и изъять цифровые следы (локальные или сетевые): различные файлы, сохранённые фотографии, документы, адреса сайтов, посещаемых пользователем, ссылки на заражённые сайты, используемые при фишинге, и путь взломщика после того, как жертвы воспользуется данной ссылкой, и др. Из каждого устройства, которым пользуется жертва или преступник можно получить данные, которые прямо или косвенно могут относиться к следствию. Смарт-часы, подключённые к мобильному телефону, могут быть исследованы как непосредственно, так и через приложение телефона. Изучив данный объект, эксперт может установить, как минимум, косвенную информацию<sup>4</sup>: местонахождение человека в определённый период времени, состояние организма (в покое или активное), ЧСС и кровяное давление. Такие сведения будут подкреплять уже имеющиеся доказательства, но не указывать ни на что прямо, если дело не касается конкретного места, например при снятии денежных средств в банкомате с чужой банковской карты.

Большой интерес представляют именно прямые доказательства. Так, когда происходят так называемые телефонные мошенничества, по SMS пользователю от имени банка приходят коды, которые, как правило, потерпевший сообщает позвонившему ему «сотруднику банка», в результате чего в лучшем случае

---

<sup>4</sup> Мещеряков В. А. Цифровые (виртуальные) следы в криминалистике и уголовном процессе // Воронежские криминалистические чтения. 2008. № 9. С. 221–232.

происходит списание со счёта конкретной суммы денежных средств, а в худшем случае – появление кредитов. В данных обстоятельствах следовательно нужно установить такие факты как способ взлома приложения, действия злоумышленника в самом приложении, причём необходимо понимать, что телефона пользователя будет недостаточно и нужно обращаться в службу безопасности банка, в которой имеется информация о получении кредита или транзакции денежных средств (адрес места перевода суммы). В приложении у пользователя такая информация тоже будет и её необходимо получить. Со смартфона имеется возможность изъять запись телефонного разговора со злоумышленником, что так же будет являться доказательством факта совершения преступления.

Помимо мошенничества, при помощи криминалистического исследования интернета вещей возможно раскрывать преступления по незаконному обороту наркотиков. Основная проблема криминалистов, экспертов, проводящих компьютерную экспертизу мобильного телефона закладчика (лица, не являющегося главным звеном в дистанционной торговле наркотиками), состоит в том, что информация, содержащаяся в устройстве, не всегда может быть доступна. Такая же проблема и с телефонными мошенничествами, хотя в том случае имеется возможность связи с банком, а вот по незаконному обороту наркотиков всё гораздо сложнее: нет возможности обратиться к какому-нибудь органу или провайдеру, который бы ответил на вопросы, связанные с личностью писавшего в мессенджере телеграмм под неидентифицируемым ником и без номера телефона. Данный вопрос касается розыска преступника, и, как показывает следственная практика, труднее найти лицо, которое торгует наркотиками через интернет, чем лицо, которое занимается телефонным мошенничеством. Трудность выхода на организатора всей цепи торговли наркотиками и иными запрещёнными веществами заключается в сложности кодов шифрования, а также в способе входа на сайты-ответвления Darknet – посредством анонимной одноранговой сети (Tor)<sup>5</sup>. Ко всему этому, оплата осуществляется криптовалютой, транзакции которой тоже сложно вычислить. Возможным вариантом установления получателя криптовалюты является выявление пути перевода средств. Для этого необходимо обладать информацией хотя бы об отправителе, а для этого надо знать хэш нужной транзакции или блока, который формируется т. н. майнерами. Получение прибыли через майнинг заключается как раз в том, что майнеры производят сложные криптографические задачи в целях создания нового блока сети транзакций. Т. е. каждый раз пути оборота криптовалюты, их коды новые, поэтому простое исследование одного технического устройства недостаточно. Нужно проводить исследования всех устройств, к которым имеется доступ у покупателя наркотических средств. Для получения нужной информации можно использовать ПК «Мобильный криминалист», UFED и другие инструменты извлечения закодированной

---

<sup>5</sup> Лукин Е. Как можно отследить транзакции биткоина // Crypto.ru [Электронный ресурс]. 03 января 2021. URL: <https://crypto.ru/mozhno-li-otsledit-bitcoin/?ysclid=lwiyettlno659578360> (дата обращения: 10.05.2024).

информации и необходимых данных для установления личности получателя и шифра хэша. Для последнего надо производить криптографические вычисления, что и отличает исследование интернета вещей от компьютерной экспертизы, предусмотренной Приказом МВД России от 29.06.2005 № 511.

При любых преступлениях, совершаемых через мобильные устройства, необходимо исследовать не только один мобильный телефон, но и подключаемые к нему вещи, так как на них может быть информация как логического, так и физического характера (результаты криптографических расчётов, данные о злоумышленниках и др.). Помимо этого, с помощью исследования всех устройств, имеющих возможность работать в подключении друг к другу, возможно установить наличие ботнета, который даёт доступ мошеннику к данным устройства. Ботнет может быть установлен как на компьютере, так и на других устройствах, имеющих соединение с тем устройством, например, со смартфоном, где расположены приложения с данными, необходимыми для совершения мошеннических действий.

Таким образом, для раскрытия и расследования преступлений, связанных с мошенничеством с использованием ботнета, незаконного сбыта веществ через сеть Bitcoin, а также ряда других преступлений необходимо внедрять в практику следственных и оперативно-разыскных подразделений исследование интернета вещей, которое заключается в детальном изучении и получении информации о личности пользователя, его контактах, местонахождении в определённый период времени, эмоциональное и физическое состояние в конкретный промежуток времени. Помимо этого, возможно получить информацию логического характера: возможность установки ботнета на какое-либо из устройств, пути его установки, хэш транзакции. Все указанные сведения необходимы для успешного и эффективного раскрытия и расследования преступлений в современную эпоху.

### Список литературы

1. Лукин Е. Как можно отследить транзакции биткоина // Crypto.ru [Электронный ресурс]. 03 января 2021. URL: <https://crypto.ru/mozhno-li-otsledit-bitcoin/?ysclid=liwiyettlno659578360> (дата обращения: 10.05.2024).
2. Мещеряков В. А. Цифровые (виртуальные) следы в криминалистике и уголовном процессе // Воронежские криминалистические чтения: Воронеж, 2008. С. 221–232.
3. Смушкин А. Б. Отдельные аспекты использования концепции интернета вещей в целях противодействия преступности // Всероссийский криминологический журнал. 2020. Т. 14. № 3. С. 453–460. DOI: 10.17150/2500-4255.2020.14(3).453-460.
4. Арбузова А., Решетникова М. Что такое интернет, кто его придумал и как он устроен: история создания // РБК Тренды [Электронный ресурс]. 15 апреля 2024. URL: <https://trends.rbc.ru/trends/industry/665dace29a7947ea2907e9cc> (дата обращения: 07.05.2024).



5. Smith G. J. D., Moses L. B., Chan J. The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach // The British Journal of Criminology. 2017. P. 259–274. DOI: 10.1093/bjc/azw096.

**Igor O. Shcherbakov**

Lecturer at the Department of Criminalistics  
Ural Law Institute of the Ministry of Internal Affairs of Russia  
(Yekaterinburg, Russian Federation)  
technikk@list.ru

**Maxim V. Uzhegov**

Student of the faculty training of investigators  
Ural Law Institute of the Ministry of Internal Affairs of Russia  
(Yekaterinburg, Russian Federation)  
uzhegov\_2002@mail.ru

## **INTERNET OF THINGS AS A SOURCE OF FORENSICALLY RELEVANT INFORMATION**

**Abstract:** The article examines the possibilities of obtaining the necessary information from devices connected to the Internet, as well as the detection of digital traces of a crime and, as a result, the formation of evidence in a criminal case. Authors focuses on the need to study the Internet of Things system, ways of committing crimes using hacking methods or any other way of influencing a device connected to the Internet; the need to pay the greatest attention to the issues of forensic research of the Internet of Things. The issues of the possibility of searching for digital traces in devices with a common domain, as well as the establishment of traces of a logical and material nature, are disclosed.

**Keywords:** the Internet, the Internet of things, digital traces, forensic research, electronic devices, computerized systems, smart devices.

**Яковлева Кристина Юрьевна**

Адъюнкт факультета подготовки научно-педагогических и научных кадров,  
Московский университет МВД России имени В. Я. Кикотя  
(г. Москва, Российская Федерация)  
kristina15.03.1998@yandex.ru

## **ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ «БЛОКЧЕЙН» В УГОЛОВНОМ ПРОЦЕССЕ**

**Аннотация:** Выделены специальные признаки и свойства технологии «Блокчейн», которые позволяют использовать её рамках уголовного судопроизводства. Представлена классификация возможностей применения технологии «Блокчейн» в уголовном процессе.

**Ключевые слова:** средства вычислительной техники; уголовный процесс; информационные технологии; блокчейн; процессуальные действия.

Информационные технологии, представляющие собой «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов»<sup>1</sup>, сегодня активно применяются в уголовном процессе. Согласно справедливому мнению О. В. Химичевой и А. А. Сумина, информационные технологии внедряются в уголовный процесс через электронные документы и развитие дистанционных форм осуществления уголовно-процессуальных действий<sup>2</sup>. Вместе с тем, различные технологии не всегда используются с благими намерениями.

Так, правоприменительной практике известны следующие продукты электронной информации, которые основаны на информационной технологии «Блокчейн», и используются в совершении преступлений:

– криптовалюта (crypto currency) – цифровые счётные единицы, учёт которых децентрализован, функционирование происходит при помощи распределённой компьютерной сети, информация о транзакциях доступна в открытом виде. Для обеспечения неизменности базы цепочки блоков транзакций

---

<sup>1</sup> Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31 (1 ч.). Ст. 3448.

<sup>2</sup> Сумин А. А., Химичева О. В. Некоторые вопросы, связанные с цифровизацией материалов уголовного дела // Сборник материалов 3-й Международной конференции «Современные проблемы уголовного процесса: пути решения» / Под общей редакцией А. Ю. Терехова. Уфа, 2022. С. 254.

используются элементы криптографии (цифровая подпись)<sup>3</sup>. Криптовалюта применяется в качестве средства вывода нелегальных денежных средств<sup>4</sup>;

– смарт-контракт (от англ. smart contract – умный контракт) – программный код, задающий компьютерный алгоритм в реестре блоков транзакций (блокчейне), в целях автоматизированного совершения и (или) исполнения сделок либо совершения иных юридически значимых действий<sup>5</sup>, также используют в хищении криптовалютных активов<sup>6</sup>.

Однако данная технология может стать эффективным инструментом в деятельности по борьбе с преступностью. Так, В. М. Елин отмечает: «применение технологии «Блокчейн» в уголовном процессе представляется отдаленной и сложной задачей, позволяющей оптимизировать деятельность субъектов и повысить качество расследования уголовных дел»<sup>7</sup>.

Отсутствие законодательного регулирования информационной технологии «Блокчейн» не является препятствием для её познания, так как появившееся многообразие авторских определений позволяет раскрыть сущность данной технологии, а также рассмотреть вопрос о целесообразности использования такой технологии в уголовном процессе.

---

<sup>3</sup> Постановление № 54-11 Межпарламентской Ассамблеи государств – участников СНГ «О Глоссарии терминов, используемых органами внутренних дел (полицией) государств – участников Содружества Независимых Государств, по вопросам противодействия преступлениям, совершаемым посредством блокчейн-технологий и криптовалют» // Единый реестр правовых актов и других документов СНГ. Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. 2023. № 77 (часть 2); Тutyнин И. Б. Химичева О. В. Применение мер уголовно-процессуального принуждения при расследовании преступлений, совершенных с использованием криптовалют: монография. М.: Издательство «Юрлитинформ». 2022. С. 14.

<sup>4</sup> Апелляционное определение Первого апелляционного суда общей юрисдикции от 26.02.2024 № 55-63/2024 (ч. 3 ст. 30, ч. 2 ст. 210, ч. 5 ст. 228.1 УК РФ) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: <https://clck.ru/3AsmbN> (дата обращения: 29.05.2024); Апелляционное определение Пятого апелляционного суда общей юрисдикции от 09.02.2023 по делу № 55-54/2023 (ч. 3 ст. 30, п. п. «а», «г» ч. 4 ст. 228.1, ч. 5 ст. 228.1, ч. 3 ст. 327 УК РФ) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: <https://clck.ru/3AsmVZ> (дата обращения: 29.05.2024).

<sup>5</sup> Постановление № 54-11 Межпарламентской Ассамблеи государств – участников СНГ «О Глоссарии терминов, используемых органами внутренних дел (полицией) государств – участников Содружества Независимых Государств, по вопросам противодействия преступлениям, совершаемым посредством блокчейн-технологий и криптовалют» // Единый реестр правовых актов и других документов СНГ. Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. 2023. № 77 (часть 2).

<sup>6</sup> Приговор Дорогомиловского районного суда города Москвы от 27.11.2023 по делу № 1-645/2023 (п. «б» ч. 4 ст. 158 УК РФ) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: <https://clck.ru/3AsqkD> (дата обращения: 29.05.2024).

<sup>7</sup> Елин В. М. Использование технологий защиты данных в деятельности правоохранительных органов // Российский следователь. 2022. № 10. С. 61–65.

Технология распределенного реестра (англ. яз. Distributed Registry Technology) «Блокчейн» (англ. яз. Blockchain – блок (block)<sup>8</sup> и цепочка записей (chain) – это:

1) с технической стороны:

- открытый обмен данных и обработка данных в некоторой распределённой сети;
- хранение данных в блоках (одна транзакция – одна запись);
- блоки связаны между собой в цепочку;
- каждый блок содержит определённую техническую информацию (метка времени, хэш предыдущего блока, хэш корневого узла, хэш заголовка текущего блока, одну транзакцию и более);
- каждый блок содержит «отпечаток» (хэш), который может быть использован для рекурсивной проверки содержимого всех предыдущих блоков;

2) с содержательной стороны:

- выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащих информацию. Является технологической основой криптовалют и их обращения, но блоки могут содержать любую другую информацию и использоваться для распределённого хранения и обработки больших объёмов данных (Межпарламентская Ассамблея государств – участников СНГ)<sup>9</sup>;

– «доступный участникам криптографически защищённый реестр, хранящий и отслеживающий данные в хронологическом порядке, создающий защищённые записи транзакций, в отсутствие модификации. Каждая транзакция заверяется криптографическими подписями участников после достижения ими децентрализованного согласия и добавляется в реестр в качестве нового. Вся зашифрованная цепь видна участникам, что делает транзакции прозрачными, при этом сохраняя персональные данные закрытыми» (А. Минина)<sup>10</sup>;

- структурированная непрерывная последовательность блоков, содержащих информацию (М. Г. Бегларян и Н. Ю. Добровольская)<sup>11</sup>;

---

<sup>8</sup> Блок – данные, которые добавляются в реестр после их проверки. После записи блока в цепочку невозможно блок удалить без замены всех последующих блоков. (Петренко А. С. Квантово-устойчивый блокчейн. СПб.: Питер, 2023. С. 21).

<sup>9</sup> Постановление № 54-11 Межпарламентской Ассамблеи государств – участников СНГ «О Глоссарии терминов, используемых органами внутренних дел (полицией) государств – участников Содружества Независимых Государств, по вопросам противодействия преступлениям, совершаемым посредством блокчейн-технологий и криптовалют» // Единый реестр правовых актов и других документов СНГ. Информационный бюллетень. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. 2023. № 77 (часть 2).

<sup>10</sup> Минина А. Блокчейн и его влияние на право // Закон.ру [Электронный ресурс]. 2 мая 2018. URL: [https://zakon.ru/blog/2018/5/2/blokchejn\\_i\\_pravo](https://zakon.ru/blog/2018/5/2/blokchejn_i_pravo) (дата обращения: 29.05.2024).

<sup>11</sup> Бегларян М. Е., Добровольская Н. Ю. Блокчейн-технология в правовом пространстве // Вестник Краснодарского университета МВД России. 2018. № 2 (40). С. 108.

– разновидность распределённого реестра, предназначенного только для добавления информации, данные в который записываются блоками с использованием криптографических алгоритмов, то есть каждый новый блок включает информацию о предыдущем блоке. Безопасность данных обеспечивается за счёт децентрализованного хранения информации и применения криптографических алгоритмов (Е. В. Былинкина)<sup>12</sup>;

– способ реализации сети распределённых реестров, в котором данные о совершённых транзакциях структурируются в виде цепочки (последовательности) связанных блоков транзакций (А. С. Петренко)<sup>13</sup>.

Предлагается применять технологию распределённого реестра «Блокчейн» в уголовном процессе в силу существования следующих её признаков, востребованных для реализации назначения уголовного судопроизводства:

– отсутствие бюрократизации, прозрачность, открытость, высокая защищённость баз данных (Л. В. Бертовский)<sup>14</sup>;

– применение криптосистемы, обеспечивающей безопасность информации криптографическими методами в части конфиденциальности, целостности, аутентификации, невозможности отказа и неотслеживаемости (Ш. А. Оцоков)<sup>15</sup>;

– возможность каждого участника обладать полноценной копией реестра (Банк России, 2017)<sup>16</sup>;

– производство синхронизации копий реестра на основе протокола достижения распределённого консенсуса, то есть соглашения среди участников на добавление новой информации (Банк России, 2017);

– доступ каждого участника взаимодействия к истории транзакций (Банк России, 2017).

Технические и содержательные сведения информационной технологии «Блокчейн» позволяют комплексно представить элементы и целый механизм данной технологии, которые полезны для её рассмотрения как возможного ресурса в уголовном процессе.

Присущие информационной технологии «Блокчейн» следующие свойства гарантированно свидетельствуют о возможном внедрении в уголовно-процессуальную деятельность такой технологии:

1) распределённое хранение данных – отсутствие единого управляющего центра, копии хранятся у всех участников технологии, кто имеет доступ;

2) целостность – невозможность изменения данных;

---

<sup>12</sup> Былинкина Е. В. Блокчейн: правовое регулирование и стандартизация // Право и политика. 2020. № 9. С. 146.

<sup>13</sup> Петренко А. С. Квантово-устойчивый блокчейн. СПб.: Питер, 2023. С. 18.

<sup>14</sup> Бертовский Л. В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. № 6. С. 227–228.

<sup>15</sup> Оцоков Ш. А. Введение в технологию блокчейн: учеб. пособие / Ш. А. Оцоков, Ю. В. Аляева. М.: Издательство МЭИ, 2023. С. 9.

<sup>16</sup> Развитие технологии распределённых реестров: доклад для общественных консультаций. Москва: Банк России, 2017. 20 с.

- 3) прозрачность – возможность видеть всю цепочку блоков;
- 4) сохранение метаданных – возможность просмотра истории изменения любых данных (невозможность отмены ранее подтверждённых транзакций или изменения данных в них)<sup>17</sup>, то есть отсутствие какой-либо возможности фальсификации доказательств и иных документов.

В Китайской Народной Республике имеется опыт применения информационной технологии «Блокчейн». Согласно «Правилам онлайн-судопроизводства народных судов Китайской Народной Республики»<sup>18</sup> (далее – Правила КНР) электронные данные могут быть представлены сторонами в качестве доказательств и быть сохранены в Блокчейне. По положительному результату проверки с помощью технологии Блокчейн электронные данные признаются непротиворечивыми. Народные суды могут предположить, что такие электронные данные не были подделаны после загрузки в Блокчейн, если только отсутствуют доказательства обратного, достаточные для признания их недействительными.

В соответствии со статьёй 19 Правил КНР «стороны могут обратиться к эксперту для предоставления заключений по техническим вопросам, касающимся электронных данных, хранящихся в Блокчейне. Народные суды могут по заявлению сторон поручить другим учреждениям проверить подлинность электронных данных, хранящихся в Блокчейне, или собрать другие соответствующие доказательства для аутентификации»<sup>19</sup>.

Итак, несмотря на то что Ц. Дун и И. Юань указывают на недостаточное формирование полной и независимой правовой системы в сфере применения электронных доказательств<sup>20</sup>, опыт КНР свидетельствует о положительном эффекте применения информационной технологии Блокчейн в уголовном процессе. К тому же, имеются правовые нормы, регламентирующие аутентификацию доказательств, содержащих электронную информацию, возможность представления доказательств, которые признают

---

<sup>17</sup> Оцоков Ш. А. Введение в технологию блокчейн: учеб. пособие / Ш. А. Оцоков, Ю. В. Аляева. М.: Издательство МЭИ, 2023. С. 8.

<sup>18</sup> «Правила онлайн-судопроизводства народных судов Китайской Народной Республики» от 18.05.2021 № 12 // The China International Commercial Court (CICC) (人民法院在线诉讼规则) [Электронный ресурс]. URL: <https://cicc.court.gov.cn/html/1/219/199/201/2208.html#:~:text=The%20right%20of%20the%20parties,litigation%20in%20any%20mandatory%20manner> (дата обращения: 29.05.2024).

<sup>19</sup> «Правила онлайн-судопроизводства народных судов Китайской Народной Республики» от 18.05.2021 № 12 // The China International Commercial Court (CICC) (人民法院在线诉讼规则) [Электронный ресурс]. URL: <https://cicc.court.gov.cn/html/1/219/199/201/2208.html#:~:text=The%20right%20of%20the%20parties,litigation%20in%20any%20mandatory%20manner> (дата обращения: 29.05.2024).

<sup>20</sup> Дун. Ц., Юань И. Сравнительный анализ электронных доказательств между Россией и Китаем // Материалы ежегодной международной молодежной научно-практической конференции (смешанный формат) «Сравнительное правоведение в странах Азиатско-Тихоокеанского региона - XIV. Отв. редактор Ю.П. Гармаев. Улан-Удэ, 2023. С. 122.

недействительными доказательства, хранящиеся на платформе информационной технологии Блокчейн.

Данные правовые положения являются мерами предосторожности и гарантируют целостность и сохранность функционирования информационной технологии Блокчейн в уголовном процессе.

На основе вышеизложенного предлагаются следующие возможности применения технологии Блокчейн в уголовном процессе России:

1. В уголовно-процессуальном доказывании при собирании доказательств, содержащих электронную информацию. В данном случае участниками могут быть представители как стороны защиты, так и стороны обвинения, а также иные участники уголовного судопроизводства.

2. В уголовно-процессуальном хранении доказательств, содержащих электронную информацию. В этом случае участниками взаимодействия являются только представители стороны обвинения и суд.

3. В восстановлении уголовного дела и материалов уголовного дела.

4. В хранении материалов уголовного дела. Данная возможность применения «Блокчейн» в уголовном процессе может рассматриваться в качестве промежуточного этапа к переходу на формирование электронного уголовного дела.

При этом польза применения информационной технологии Блокчейн в хранении материалов уголовного дела заключается в следующем:

- исключается подмена страниц вынесенного решения, оформляемого постановлением следователя (дознателя);
- отсутствуют возможности потери и утраты материалов уголовного дела;
- обеспечивается высокая степень защиты фиксации хода следственного действия от случаев подделки подписей участников уголовного судопроизводства и фактов фальсификации доказательств в уголовном деле.

Таким образом, на современном этапе развития информационной технологии Блокчейн сформировался ряд возможностей для её применения в уголовном процессе. Основой этому является ряд признаков, свойств и выделенных элементов полезности применения криптографического инструментария защиты электронной информации в уголовном процессе. Существующая нормативно-правовая, теоретическая и технологическая база позволяет осуществить внедрение информационной технологии Блокчейн в уголовный процесс.

### **Список литературы**

1. Бегларян М. Е., Добровольская Н. Ю. Блокчейн-технология в правовом пространстве // Вестник Краснодарского университета МВД России. 2018. № 2 (40). С. 108–110.

2. Бертовский Л. В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридический практики. 2017. № 6. С. 226–230.

3. Былинкина Е. В. Блокчейн: правовое регулирование и стандартизация // Право и политика. 2020. № 9. С. 143–155. DOI: 10.7256/2454-0706.2020.9.33614

4. Дун. Ц., Юань И. Сравнительный анализ электронных доказательств между Россией и Китаем // Материалы ежегодной международной молодежной научно-практической конференции «Сравнительное правоведение в странах Азиатско-Тихоокеанского региона – XIV» / Отв. редактор Ю. П. Гармаев. Улан-Удэ, 2023. С. 122–127.

5. Елин В. М. Использование технологий защиты данных в деятельности правоохранительных органов // Российский следователь. 2022. № 10. С. 61–65.

6. Минина А. Блокчейн и его влияние на право // Закон.ру [Электронный ресурс]. 2 мая 2018. URL: [https://zakon.ru/blog/2018/5/2/blokchejn\\_i\\_pravo](https://zakon.ru/blog/2018/5/2/blokchejn_i_pravo) (дата обращения: 29.05.2024).

7. Оцоков Ш. А. Введение в технологию блокчейн: учеб. пособие / Ш. А. Оцоков, Ю. В. Аляева. М.: Издательство МЭИ, 2023. 92 с.

8. Петренко А. С. Квантово-устойчивый блокчейн. СПб.: Питер, 2023. 320 с.

9. Сумин А. А., Химичева О. В. Некоторые вопросы, связанные с цифровизацией материалов уголовного дела // Сборник материалов 3-й Международной конференции «Современные проблемы уголовного процесса: пути решения» / Под общей редакцией А. Ю. Терехова. Уфа, 2022. С. 253–258.

10. Тутьин И. Б. Химичева О. В. Применение мер уголовно-процессуального принуждения при расследовании преступлений, совершенных с использованием криптовалюты: монография. М.: Издательство «Юрлитинформ». 2022. 144 с.

**Yakovleva Kristina Yurievna**

Postgraduate student of the Faculty of Training of Academic and Research Personnel  
Moscow University of the Ministry of Internal Affairs  
of Russia named after V. Ya. Kikot  
(Moscow, Russian Federation)  
kristina15.03.1998@yandex.ru

## **THE POSSIBILITIES OF USING BLOCKCHAIN TECHNOLOGY IN THE CRIMINAL PROCEDURE**

**Abstract:** Special features and properties of the Blockchain technology have been identified, which allow it to be used in criminal proceedings. The classification of the possibilities of using Blockchain technology in criminal proceedings is presented.

**Keywords:** computer technology, criminal procedure, information technology, blockchain, procedural actions.



*Научное издание*

## **ТЕХНОЛОГИИ XXI ВЕКА В ЮРИСПРУДЕНЦИИ**

Материалы  
Шестой всероссийской научно-практической конференции

(г. Екатеринбург, 24 мая 2024 года)

Компьютерная вёрстка: Д. В. Бахтеев

Корректоры: С. А. Кошкина, А. Д. Цветкова

Рисунок на обложке: Андрей tramdreу Негруль

**АНО «Центр содействия развитию криминалистики «КримЛиб»**

**Основной сайт:** [hub.crimlib.info](http://hub.crimlib.info)

**Канал:** [t.me/crimlib](https://t.me/crimlib)

[ae@crimlib.info](mailto:ae@crimlib.info)

**Уральский государственный юридический университет  
имени В. Ф. Яковлева**

620137, г. Екатеринбург, ул. Комсомольская, 21  
[usla.ru](http://usla.ru)

**Союз криминалистов и криминологов**  
[crimescience.ru](http://crimescience.ru)

**Проект «РИТВУС»**

**Подписано к использованию: 17.06.2024**

**Согласно п. 1. ч. 2 ст. 1, п. 1 ч. 4 ст. 11**

**Федерального закона от 29.12.2010 № 436-ФЗ  
маркировке не подлежит**

**Электронное издание**

Минимальные системные требования: ОС Windows XP/Vista/7/8/8.1/10/11, RAM  
512 МВ и выше, необходимо на накопителе: 4,5 Мб, CD/DVD- привод,  
программные средства для просмотра pdf-файлов  
Объем издания: 4,5 Мб, 1 электрон. опт. диск (CD-ROM).